



NarrowCast Group, LLC ●●● 10400 Linn Station Road, Suite 100 ●●● Louisville, KY 40223

## IT Business Edge Definitions

### Agile Development

#### Definition

"Agile methods assume that change is inevitable and seek to incorporate change, not resist change." –Doug Mow, Senior VP of Marketing, Exigen Services

When someone refers to something in the software development world as "agile" or describes something as adhering to "agile development" practices, they are talking about iterative development methodologies where deliverables are submitted in stages. Iterative methods emphasize a development process where cross-functional teams collaborate intensely and requirements and solutions change over the course of the development cycle. Tasks are broken out into "chunks" and development takes place in shorter "sprints" or "timeboxes" that differ from other iterative methods in that delivery time is a matter of weeks and not months.

Agile methods also differ from traditional "waterfall" methods in several ways and [offer some clear benefits](#), according to Social, Agile and Transformation blogger Isaac Sacolik:

- Less up-front business involvement since development teams can get to work quickly on the most critical features and risky technical areas
- Frequent delivery, better execution by way of constant feedback during iterations
- Improved IT/business alignment through up-front prioritization by stakeholders at the start of each iteration.

Depending on how things are going, and how things are working, different elements (requirements, tasks, etc.) can be altered as the process progresses. This flexibility allows team members to move, switch, and manipulate the different iterations as the project progresses.

That's the agility from which the method gets its name. Agile "[values flexibility, simplicity and getting tasks accomplished quickly](#)."

Agile development shares principles found in other modern operations management approaches such as Six Sigma and "lean" manufacturing. Among these principles:

- Eliminate wasteful practices
- Minimize errors

- Empower workers
- Add customer value

These principles are also found in the Toyota Way framework and form a part of the Toyota Production System (commonly referred to as TPS). Other Agile devotees include engineers for General Electric's SupportCentral Network; IBM has a growing community of developers taking part in their Agile@IBM initiative.

Generally, agile methods stress the importance of frequent inspection and adaptation ("[Go See](#)"), teamwork, best practices that allow for high-quality with rapid delivery, accountability and the proper alignment of customer needs with company goals.

Well-known agile methods include:

- Agile Modeling
- Agile Unified Process
- Extreme Programming
- Scrum ([identified as the most popular by respondents](#) to a Forrester Research survey, according to IT Business Edge blogger Ann All)

## **Business Applications**

While primarily applicable to software development project management and maintenance, agile techniques have been created and adapted for the development and production of other products such as motor vehicles, as with Toyota. Agile methods have been successfully applied to the banking and investment, aerospace, and other manufacturing industries.

## **Concerns and Criticism**

While evidence of successful, large-scale agile projects exists, larger numbers of developers often negatively affect success, as does a lack of physical proximity or "co-location" (since communication and collaboration are critical), although strategies for addressing both have been developed. According to Ann All:

"Whether a project is in-house or outsourced, Agile requires a high degree of collaboration between IT and the business, something that not every organization is prepared to offer."

This means safeguarding against agile-related risks such as the tendency for agile projects to be short of proper oversight, says IT Business Edge commenter Aleks Buterman. A lack of oversight tends to increase complexity due to duplication of effort.

Agile projects are also more likely to fail if the processes are forced on software developers; larger organizations often have difficulty making the transition from traditional methods (i.e. "waterfall") to agile ones for this reason. From a project accounting standpoint, agile projects can be difficult to forecast in terms of cost. Foes of agile methodologies often point to the failure of Chrysler's C3 project as a prime example of failed implementation by chief agile proponents.

Moreover, projects developed using agile methodologies may not realize the full benefits of using them if teams are composed of less experienced or skilled developers. Agile projects are most likely to succeed when the teams consist of fewer than 20 members, are located in the same geographic area (co-location), and are comprised by seasoned software developers.

Steve Hardin, Vice President of Software Engineering at IT Business Edge, has seen this borne out in projects he's undertaken:

"Agile isn't a fit in all companies. It's easier to implement using small teams. And, for some outsourced projects, waterfall methods are easier because, with those methods, everything is

broadly documented in advance. For us, agile methods have been faster in terms of getting code out the door. With my team, we saw the initial requirements, did our mock-ups, and then got user feedback much sooner in the process. We were faster to working code because we didn't have to do a lot of upfront documentation. Documentation written at the outset of a project often becomes obsolete very quickly as it doesn't reflect reality. Agile doesn't mean "no documentation." It does mean less documentation because you are actually working on the product. What documentation you write should evolve as the project evolves, not become an outdated afterthought. This way, you keep documentation simple so you can focus on the function and get that critical user feedback.

Concerns regarding co-location and scale have resulted in many businesses taking a hybrid approach to adopting agile methods (an approach that Hardin is also considering for future projects). The Forrester survey seems to bear this out, pointing out that most development teams use several different agile methodologies "embracing agile as an ethos or philosophy and cherry-picking the best bits...to develop a formula unique to their own situation."

Al Gibson, who cautions against improper or inappropriate adoption of agile in comments in Ann's "Business Analysts Need to Get More Agile" post (and uses the C3 case as illustration of [failed agile implementation](#)), advocates a hybrid strategy, having seen positive results (read: quashed developer rebellion) from a "sensible" switch from a hastily pushed agile management method to a marriage of agile and traditional methods.

As the need for "sensible" mixtures of old and new approaches grows so do sensible attitudes like Mow's. Echoing Hardin, Mow says that, sometimes, agile just cannot work:

"[In] situations where the business community simply is not accessible or collaborative...there's no sense in trying to enforce change if the organizational environment is unwilling to accept it. You'll incur more risk than you've managed to reduce."

Even if agile development methodologies cannot or should not be implemented across a particular business, teams that use traditional development methods can benefit from newer techniques like incremental feature releases and increased user feedback.

## Android

### Definition

Android is a Linux-based mobile software platform and operating system developed by Google and the Open Handset Alliance. It's based on open standards and is open source.

T-Mobile released the first commercially available Android-based phone in the last quarter of 2008. The handset, which supports T-Mobile's 3G network, received [FCC approval](#) in August 2008.

Samsung, HTC and LG also [plan to release phones](#) on the Android platform.

### Business Applications

Android will ship with the typical smartphone applications, including an e-mail client, SMS program, calendar, maps, browser and phone book.

[Applications for Android platform](#) will be developed in the Java programming language; so theoretically, companies could develop their own applications for mobile phones. Again, theoretically, these applications could run on other devices as well, though some experts warn this would be harder to do in practice.

In May 2008, Google offered \$25,000 to programmers who created the 50 best applications in its Android Developer Challenge, however, only a few of the applications had tangible business use (<http://www.itbusinessedge.com/blogs/cip/?p=352>).

### Deployment Concerns

Because the Android framework is open source, [some experts](#) have raised concerns about security. [Others](#) believe it will be more secure than the iPhone.

To address security concerns, [Google publicly asked](#) the mobile security community for help in identifying bugs when releasing its Android software Development kit.

### Technical details

Android includes an operating system, middleware and key applications. It's based on a Linux kernel, version 2.6. The platform [is being released](#) under Apache2 license, even though the underlying Linux kernel is licensed under the General Public License version 2 (GPLv2).

Android will run on Windows, Linux and Mac systems. It also will support variety of connectivity technologies, including Bluetooth, Wi-Fi, EDGE and 3G.

Applications will be developed in Java using the Android Development Kit, which is available for free download (<http://code.google.com/android/intro/installing.html>). Android also includes the Dalvik virtual machine and a set of C/C++ libraries used by various components of the Android system, according to Google's online [Android documentation](#).

## API

### Definition

An application programming interface (API) is a set of routines, protocols, and tools used to build software applications (a.k.a. programs). [Operating systems use APIs](#) to provide a way for applications to use OS resources; APIs can also be used to extend the functionality of other applications, provide remote services to Web sites or allow Web sites to interact with one another using other Web technologies (e.g. [Open APIs](#)). They are [increasingly critical in the development](#) of (and add to the complexity of developing) multi-platform mobile applications.

### Business application

APIs help software programmers build applications more easily by providing all the “parts” they need to put the application together. While this is good for programmers, it is also beneficial to shortening learning curves for users, as it results in applications that behave consistently within an operating environment (for example, in the [Windows Operating System](#), applications built using a common API will have similar interfaces).

In short, the use of common APIs gives your company’s software offerings a consistent look and feel, making your coders look good and your users feel good. Open APIs allow for extensibility and integration among Web applications and open up possibilities for new partnerships.

### Concerns

As IT Business Edge’s Integration blogger [Loraine Lawson](#) points out:

“Language-independent APIs, which can be accessed by any number of programming languages, are broadly preferred over language-dependent APIs.”

In addition, open APIs are gaining popularity, as third-party developers adopt them in order to [build apps for sites like Google](#) or Facebook as well as mobile platforms like the iPhone. Businesses have been “shy about open APIs,” according to Lawson, but [they are warming up quickly](#):

“... open APIs have become an increasingly vital story for Web startups and traditional firms alike to cost effectively partnership, expand the reach of their products (and especially their data), and drive their network effect deeply across the Web. It’s now almost uncommon to see a new Web product that doesn’t sport a shiny new API so that other online products can integrate the pieces they like into new experiences and offerings. In short, APIs allow a Web application or online business to have thousands of points of presence in other products, instead of just one.”

## Application Deployment

### Definition

Application deployment aims to improve asset utilization, operational efficiency and business agility for enterprises.

### Business Applications

As data loads get heavier and heavier, many enterprises are seeing application performance suffer. Helpful to application deployment, the rise of application-delivery platforms has helped somewhat. But many of the leading systems are not flexible enough to meet changing business demands. For instance, Seattle's F5 networks offers a solution—[F5 Boosts Application Delivery Platform](#)—not only to trim the number of controllers needed in the data center, but to support some of the newer resource-hungry services such as Web-application firewalls, content transformation and application-specific acceleration. Shipments of F5's BIG-IP 6900 platform are expected by the end of 2008.

### Deployment Concerns

The real effort at the moment is establishing third-party relationships aimed at smoothing out many of the deployment issues. VMware, the market leader in virtual desktops, announced its [vClient Initiative](#), to establish a "universal client" that will be available to users from any end point. VMware customers will be able to use a tool called [SmartClone Volumes](#) that streamlines virtual desktop deployments by replicating volumes and data sets without having to add storage to ease multiple system images.

### Technical Details

A recent report from IDC claims that with the current global economic downturn, corporations will increasingly turn to desktop virtualization as a cost-savings measure. VMware stands to benefit.

Meanwhile, IBM wants to show that it can provide a DV platform without help from Microsoft. The company has teamed up with Canonical and Virtual Bridge to provide a Linux-based system that the company says will cost half as much as a comparable Windows solution. The system bundles IBM's Open Collaboration Client Solution with Canonical's Ubuntu Linux and VB's virtual desktop software.

## Application Performance Management

### Definition

Seen as a business-intelligence process, [application performance management](#) is usually a back-burner issue around the office. A lot of companies will say they're doing performance

management, but their efforts usually end up approaching the level of passing around a bunch of spreadsheets that somebody types numbers into.

## **Business Applications**

There are automated systems out there that will grab data from different sources and aggregate them and roll them up into scorecard tools that can easily be seen by the whole team. These tools support collaboration.

Businesses that do invest in application performance infrastructure spend an average of \$96,000 per year and can mitigate the risk of losing up to \$117 million per year. The best approach is not to shell out for marquee systems that address only the major app performance issues, but to install a wide range of capabilities designed to manage full application lifecycles.

## **Deployment Concerns**

64-bit corporate performance management (CPM) applications provide a several order of magnitude improvement in deployment options at reasonable costs. With the CPMs, you may have a several order-of-magnitude improvement in the underlying architecture that will allow software providers to do some new things they never would have considered in the past. The door will be open to new strategies and approaches to begin experimenting with and devising new functionality and capabilities in anticipation of the increasing need for more agile, collaborative and holistic performance management.

## **Technical Details**

The experience of Japan's Daiwa Securities offers an example of the kind of improvement that souped-up application performance can bring. The company had a proprietary system that supported more than 120 applications for about 250 employees, but frequent crashes and poor tech support would knock the system out on a weekly basis for more than an hour at a stretch—an eternity in the securities business. The company recently migrated to Red Hat's JBoss Enterprise Application and Portal Platforms, delivering an instant savings of \$300,000 in licensing and hardware costs, and has cut application compiling and delivery times from about 15 minutes to a few seconds.

## **Application Servers**

### **Definition**

An [application server](#) is a software module within a distributed network that contains the APIs and business logic needed by standard applications. The application server is usually considered one of the three legs of a typical business application, the other two being the graphical user interface (GUI) and the database/transaction server.

Most application servers are based on the [J2EE](#) or [Java EE 5](#) formats, including a number of WebSphere releases from BEA, and other from Red Hat, Oracle, Sun and SAP.



## Business Applications

Any number of functions can be relegated to the application server, with the goal being to improve network performance by relegating application traffic to its own tier. Common uses include logic centralization to facilitate configuration changes and updates, as well as security enhancement by focusing on only one point of data access and application management.

An application server can also be used with a [Web server](#) that supports a browser-like interface to simplify the transfer of data to and from the app server.

## Deployment Concerns

Supporters believe the use of an application server enhances [collaboration](#) among developers and improves the application development process, saving money in the long run. Establishing a smooth-running environment can be tricky at times, though, considering all software written for the application must integrate with the server environment and all data is distributed back out must contain client code. These problems are not overwhelming, but they do point up to some of the challenges involved with network collaboration.

Another problem is the lack of integration between Java- and non-Java-based servers. This increases the complexity of many application integration platforms like [Business API](#) and [Web Services Interoperability](#) in order to accommodate the different formats.

## Technical details

The inner workings of application servers vary widely, as each developer has been largely free to set their own definitions. Some are open source systems, like [JOnAS](#) and [Base4](#), while others conform to leading enterprise platforms, such as the Java Enterprise Specification.

Microsoft has established its own platform called the [.NET Framework](#). It incorporates a number of Microsoft modules like the [Windows Communication Foundation](#) and [Internet Information Services](#).

## Anti-spyware

### Definition

Anti-spyware is software that removes or blocks software that is installed on a personal computer without the user's knowledge.

### Business applications

Anti-spyware software is an important element in a company's security strategy. Without it, businesses are susceptible to data and productivity loss as a result of spyware-infected PCs. Businesses should consider implementing anti-spyware on clients to block the installation of spyware and have anti-spyware-removal tools for cleaning infected machines. There are



many well-known anti-spyware programs, and major antivirus vendors have also added anti-spyware to their antivirus products.

## **Concerns**

Not all anti-spyware products are created equal. Some give more than they take away. Rogue anti-spyware programs warn users through Web banners and pop-up ads that their machine has become infected and promise to remove the spyware. However, downloading the rogue software does not remove any spyware and may, in fact, add spyware to the machine. Experts recommend prohibiting the use of freeware that claims to be anti-spyware unless its legitimacy has been verified.

While legitimate anti-spyware software plays a significant role in protecting systems, it is not the end-all. Best practices dictate that companies discourage the use of Internet Explorer for surfing the Web, which is at greater risk for spyware infections and ActiveX vulnerabilities than the less popular Opera or Mozilla Firefox Web browsers. Companies may also block access to Web sites associated with spyware by configuring their network firewalls and Web proxies accordingly. The use of shareware, which is also often associated with spyware, might also be prohibited.

## **Technical details**

Anti-spyware software can be proactive or reactive in its approach to battling spyware. It can provide real-time protection against spyware by scanning incoming network data and blocking attempts to install spyware. Or anti-spyware can periodically scan a machine to detect and remove spyware that has already been installed.

Similar to antivirus, there are also two ways in which anti-spyware can detect malicious software. It can take a rules-based approach, or it can rely on signature or definition files based on current spyware programs. Of course those signature files need to be continually updated. While updates are not necessary for rules-based anti-spyware programs, the user must ultimately determine whether a configuration change flagged by the anti-spyware is appropriate.

## **Antitrust**

### **Definition**

Antitrust is a term used in reference to a series of [federal laws passed](#) to break up monopolies, end unfair trade practices, and promote competition among businesses. The three landmark antitrust laws are the Sherman Antitrust Act of 1890, the Clayton Antitrust Act of 1914, and the Federal Trade Commission Act of 1914. Many other states have even adopted their own antitrust laws in addition to these federal laws.

### **Business applications**

Antitrust laws were established to break down large monopolies and encourage competition among businesses. The [Federal Trade Commission](#) enforces these laws to help guarantee that

businesses and consumers both avail from increased options, lower prices, and competition to provide higher quality services and products.

## **Concerns**

There are a couple of major concerns when it comes to antitrust laws—that they punish large, successful businesses and that they are very difficult to define and enforce. The argument for the former is that sometimes companies that are deemed “monopolies” are actually just the leading example in their field and other companies just haven’t created products that are on par to compete (i.e. [Microsoft](#)). Also, most cases of antitrust violations are only enforced after a civil enforcement action is brought about or after a private party files a lawsuit. In such cases the [Department of Justice](#) investigates the claims and works with other agencies to gather evidence and enforce any violations.

## **More information**

In the past decade, there haven’t been many antitrust cases in the courts. To learn more about recent antitrust cases, you can visit the [Antitrust Case Browser](#) or the U.S. Department of Justice [site](#).

## **Antivirus**

### **Definition**

Antivirus is software that scans a personal computer for evidence of malicious software. When it finds a file infected by a virus or other type of malware, antivirus software either neutralizes or eliminates the file to prevent the infection from spreading and damaging systems.

Antivirus programs can protect systems against a variety of malicious code, including worms, Trojans, spyware, rootkits and more.

### **Business applications**

Businesses should deploy antivirus on all personal computers as one of many layers in a [defense-in-depth](#) security strategy. Many security vendors offer antivirus products, and while there are small variations in the way they respond to viruses, antivirus products ultimately perform the same function. Some of the more popular vendors include McAfee, Symantec, CA and Sophos. When choosing an antivirus vendor, businesses may consider price, recommendations, features or availability.

### **Deployment Concerns**

Stand-alone antivirus software is no longer enough to protect systems against the barrage of malware that constantly attempts to undermine systems. Experts recommend deploying a [suite of applications](#), including antivirus, for more complete protection against malware.

Antivirus software also has been found to have its own vulnerabilities that could pose a danger to the very systems it's meant to protect. A consulting firm found that [many antivirus programs can be exploited](#) through vulnerabilities within the malware-scanning process known as parsing. That's yet another good reason to deploy defense-in-depth.

## **Technical details**

Antivirus software can perform manual and automatic scans. Best practices dictate running a complete scan immediately after installing the software, configuring full automatic scans to run periodically and running manual scans on incoming files (for example, e-mail attachments or Web downloads).

Antivirus programs can also use two methods for detecting malware: matching signature files and heuristic analysis. When matching signature files, antivirus software compares the code in a file to a dictionary of known virus signatures. When it finds a match, the antivirus software repairs, deletes or quarantines the file. This type of antivirus software must be regularly updated to include the latest virus signatures. New viruses are constantly being created so antivirus vendors are challenged to keep up by creating signatures for each new virus.

Heuristic analysis is the examination of suspicious behavior to determine whether it's being caused by a virus. For example, if one program attempts to write data to an executable program, the antivirus software may raise a warning to the user. Because this method does not rely on current signatures, it is used to detect new viruses for which signatures are not yet available, and variants of old viruses. However, heuristic analysis requires user action when suspicious behavior is flagged. That can be a problem if the antivirus software has a high false-positive rate and users begin to ignore the warnings.

## **Application Security**

### **Definition**

Application security is a collective term that refers to the efforts throughout an application's life cycle to identify and fix vulnerabilities in the code that could put systems and data at risk. Various procedures, hardware and software can be used to detect and fix flaws in the design, development, deployment, upgrading or maintenance of an application.

Traditionally, application security has been an afterthought, with businesses scanning their Web and other applications only after they "go live." However, [according to Gartner](#), that will change as businesses become increasingly aware of the significant class of vulnerabilities that applications can harbor.

### **Business Application**

Network security efforts alone cannot protect applications from the many vulnerabilities that riddle code. Whether building custom applications in-house or purchasing vendor-built

software, businesses should plan an application-security strategy that enforces security practices throughout the application's life cycle.

Begin by identifying business assets and how the application will use them, keeping in mind that applications only control the assets or resources that are granted to them. Next, identify the vulnerabilities in the application and the threats that can exploit them. Based on the value of the asset and the risks posed by vulnerabilities and threats, determine an appropriate countermeasure. This may include accepting the risk without deploying a countermeasure or choosing to avoid the risk altogether by turning off the functionality or removing the piece of code causing the vulnerability.

### **Deployment Concerns**

Many businesses fail to recognize the importance of application security, despite the fact that [8 out of 10 Web sites have security holes](#), according to Jeremiah Grossman, CTO of White Hat Security. They mistakenly depend on traditional vulnerability-assessment tools to identify weaknesses in their applications, but that just isn't enough.

Businesses also generally lack the financial and technical resources to do application security. If this is the case, consider application detection/scanning services by companies such as White Hat Security, SPI Dynamics and OmniTI.

### **Technical details**

Application security can be achieved through a variety of countermeasures that should be used together. Procedures should be integrated in each step of the application-development process to avoid expensive fixes and delays in the application release. Software application-security scanners can be used to test application code for vulnerabilities.

Once the application is deployed, businesses may consider also deploying an application firewall. Where an intruder may get past a network firewall, a software application firewall can stop the execution of potentially malicious code that could exploit vulnerabilities in the application. Hardware countermeasures, such as a router, sit on the network. A router can prevent the IP addresses of computers using applications from being visible on the public Internet. Other countermeasures include antivirus, anti-spyware, encryption, network firewalls and authentication systems.

Applications can be vulnerable to a variety of threats and attacks. The Open Web Application Security Project publishes the [top 10 Web application-security problems](#), which can be helpful to businesses when determining a strategy for application security.

Among the most common application-security threats are input validation attacks, such as buffer overflows, SQL injection and cross-site scripting. Input validation involves checking the data entered into forms -- for example, the address field in a Web contact form -- to ensure that the

data entered is appropriate for that field and does not include characters that could exploit the application.

Other application-security threats include eavesdropping, elevation of privilege, session hijacking, data tampering, denial of service and information disclosure.

## Blade Servers

### Definition

A [blade server](#) is a mini version of a full-sized server that contains all of the computing resources of a full server but not all of the power and cabling. Those functions are handed off to a [blade enclosure](#), which allows for denser configurations than traditional server architectures and thus provides greater computer power per square foot in the datacenter.

### Business Applications

Blades can perform all of the functions of a standard server, and can therefore serve the entire range of business applications, from [CRM](#) and [Business Intelligence](#) to security, [web hosting](#) and application development.

Being small and compact, they are ideal for [clustered server architectures](#). They are usually hot-swappable, allowing for easy scalability.

Blades can also be devoted to specialized purposes, such as switching, routing and storage. Indeed, it is common practice to devote one blade in the enclosure to a specific function so the others can focus on data and application processing.

### Deployment Concerns

The chief concern with blades is [power consumption](#). While individual blades draw less power than standard servers, the fact that you can pack three times as many blades onto the same floor space increases the power draw for both processing and heat dissipation. The blade itself does not include a fan, so a fully loaded enclosure has to work extremely hard to keep the devices from overheating.

Newer blade enclosures feature more power fans and [advanced power and cooling management technology](#) to alleviate the problem, although it is still risky to load many enclosures past the halfway point. Some enclosures are starting to feature water-cooled designs.

Most blade servers are built on an open platform, theoretically allowing them to be mixed and matched in multi-vendor environments. In practice, though, this is more difficult than it sounds, with many users opting for single-vendor deployments for improved management and connectivity.

### Technical details

A blade enclosure can hold up to 128 blades, compared to a standard rack of 42 servers. A typical blade will contain processors, a small amount of memory (usually an [ATA](#) or [iSCSI](#) drive), an integrated network controller and possibly an HBA or some other I/O port device.

More information on blade servers can be found at [blade.org](http://blade.org).

## Business Continuity

### Definition

[Business continuity](#) is a daily process by which an enterprise ensures that its most critical functions are accessible by those who need them in case of some type of disruption. The [activities covered in the business continuity](#) structure might include call center management, system backups, or any daily chore or service on which the business relies to run smoothly.

A disaster recovery plan is not the same as daily business continuity; however, a plan for recoverability in the instance of a disaster may be part of the overall business continuity plan. A well-developed business continuity methodology would also include such components as: policies, standards, procedures, organization structure, security management, change management, document management and service level agreements.

All companies should take time to create a business continuity plan. Before such a plan can be created, though, the management must identify the most [critical areas of the business](#) and which must be protected and made accessible in the event of a crisis. Other considerations include budgeting for the business continuity plan itself, considering outside help from a company that provides business continuity planning (BCP), and identifying the various areas of the business that should be involved in the planning.

### Business Continuity Planning

A [comprehensive business continuity plan](#) can ensure that a company continues to bring in revenue even during interruptions such as power outages, loss of key employees, disruptions in service from outside providers, or any other problems a business could encounter. Creating such a plan will involve input from many areas of the company, and the scope of the plan will depend upon the size of the company and the way it performs its business.

The end result of [business continuity planning](#) should be a printed reference manual that various business areas can utilize when necessary. The manual itself will vary in size and scope—a printed document for a smaller business may contain basic information and be stored offsite in case of emergency, while a larger company might require several volumes for each area affected by the crisis and be available from various sites and possibly online. Either way, the manual should be easy to use and mesh with the company's disaster recovery and risk management strategies.

There are five main phases that BCP manual creation should include:

- Analysis of business impact, threats, and potential scenarios that would require the manual's usage.
- Determining solutions for the crisis command structure and secondary worksite location (if necessary); plus how communications, data, hardware, and software will be supplied and used at the secondary site.
- Implementation of any elements determined in the solution phase.
- Testing the plan and achieving organization acceptance among the various company areas affected.
- Maintenance of the manual through awareness training of staff who hold critical roles along with periodic testing and verifying of procedures as outlined.

## Concerns

One of the largest concerns when creating a [business continuity plan](#) is that of cost. Larger companies will require more money to create, test, and utilize a comprehensive business continuity plan. However, when you consider how much money a company could lose if it experienced disruptions of service, paying for a well-created [plan for continuing business during a crisis](#) may seem like money well spent to the upper management.

## Technical Aspects

As most businesses rely on various areas of technology to run properly, most business continuity strategies mainly involve IT. A well-developed plan would likely involve ensuring Web site availability, providing staff with Internet and e-mail access, and providing access to necessary computer systems and software.

A relatively new technology to the business continuity plan is [virtualization](#). Many larger companies utilize virtualization technologies for storage and to supply applications to users. Virtualized machines can often be recovered more quickly since copies can be stored offsite in case of a server failure, which makes the technology ideal for many [business continuity scenarios](#). However, the technology is still in its infancy and many applications may not run in a virtual environment.

## Client-Server Network Application Model

### Client-Server Network Application Model - The Value of Enterprise Resource Planning Software

Enterprise resource planning is a very popular class of enterprise applications represented by such companies as Oracle, Peoplesoft, Baan and SAP. The software is comprised of various modules for managing different company departments while integrating them as well. The current application model is described as a three-tiered design that describes the flow of traffic between client and servers. The application is comprised of a client software module, an application server module and a database server module. The three-tiered model has the application and database modules residing on different server machines.



There is significant performance improvement with the three-tiered model, since all application and database transactions can be co-located at a high-speed data center with Gigabit campus switches. The client software is engineered to send an efficient smaller request, which is 2-3 Kbytes across a WAN link to an application server.

The application server processes that request by sending a specific query to the database server, which will be on the same campus segment. The database finds the database record and returns that to the application server. The application server then sends an SQL reply with that information to the client across the WAN.

This model was designed for the most effective utilization of circuit bandwidth, which has the most effect on company costs and application performance. As well, co-locating the application and database servers on the same campus segment and on different machines allows for scalability and performance.

The campus Gigabit links at the data center are at least 10x faster than the WAN circuits. That and splitting the application and database modules allow for scalable databases and higher-performance application servers. With both modules running on one server, there would be an upper limit at which those modules would have to be separated. Future developments with ERP applications will focus on making a client software module that requires even less bandwidth than the current 3 Kbytes for a faster response time and cost-effective bandwidth usage.

## Client System Configuration

### Definition

The only way organizations can be assured that their network infrastructure is configured to deliver the required volume and quality of traffic in and out of their data centers is by fitting all of the elements in a consolidated and automated management system.

In addition, there are growing requirements stemming from compliance standards and green thinking.

### Business Applications

Thin clients are cheaper, easier to manage and use less energy than the standard business desktop. But, now, what once was a drawback, an inability to process large multimedia files, may no longer be a problem with beefed-up processing and newly redesigned software from the major vendors. Some experts suggest that growth is coming in this industry because of these [“green and cost-effective alternatives to expensive and difficult to manage PCs.”](#)

Other opportunities include HP’s [Virtual Client Essentials](#) and the [Wyse Thin Client OS](#) version 6.3 that includes a new collaborative processing architecture that can detect heavy data applications on the server, such as video and graphics processing, and shift that over to the client.

### Technical Details

Big data centers, such as Microsoft, Google, Yahoo, now have phenomenal purchasing power and they buy energy-efficient configurations. Server OEMs such as IBM, Dell and HP, in turn, take those and sell them to other people. The interesting part is, all server OEMs have data-center [best practices] areas now. They work with companies and ask, "What is the most efficient area for your data center?" That is a way to try to win sales.

You need to have centralized purchasing of the servers that goes across all the different departments. The inefficiencies come from all the different departments buying what they want as opposed to one department being a resource for others and saying, "Here is the energy-efficient version." (See [Unleashing the Friendly Green-Eyed Monster in Data Centers](#).)

## Cloud Computing

### Definition

Cloud computing is the ability to draw IT resources from an internal or external, third-party source using either Internet-based or local-area infrastructure. The cloud is essentially the [Software-as-a-Service \(SaaS\)](#) model expanded to include hardware-driven functions like storage and processing.

While the concept dates to the late 1960s, the modern cloud movement began in 2002 with the launch of Amazon.com's [Amazon Web Services](#). The company followed up with the [Elastic Computer Cloud](#) (EC2) in 2008, and has since been joined by Google, Microsoft and others.

### Business Applications

Applications range from server and storage services to application development/testing to the applications themselves, like [ERP and CRM](#). In fact, it is conceivable that enterprises will soon be able to out-source virtually all their IT needs to the cloud, avoiding the cost and complexity of building an IT network from the ground up.

Likewise, established enterprises could use their existing networks to provide cloud services "behind the firewall," that is, a [private cloud for strictly internal purposes](#). This would improve management capabilities and allow resources to be dynamically shifted to meet rising and falling data loads, at once eliminating current silo architectures and the need to over-provision resources to meet peak demand. Internal clouds can also be [leased to third parties](#), turning IT from a cost center to a revenue generator.

### Deployment Concerns

Security and reliability are the two major issues. [Cloud-based storage](#) is a particular concern, considering it places institutional knowledge under the control of someone else.

On the security front, the main issue is the fact that [users are not passing through the standard sign-on and Web access protocols](#) before hitting the cloud. Mobile and remote users in particular can often bypass enterprise network security entirely.

As for reliability, cloud access is only as good as the Internet service it's carried on.

## Technical details

The cloud is essentially an abstraction of the existing Internet infrastructure. As such, it requires [client-side hardware and software](#) tied to legacy computing infrastructures and ever-shifting application, virtualization and middleware software layers.

Many cloud providers have adopted the “[utility computing](#)” model of delivery in which IT resources are distributed to users much as electricity and telephone service.

Key enabling technologies include [high-speed networking](#) bolstered by [10 GbE](#) in the enterprise, and advanced [Application Programming Interfaces \(APIs\)](#).

## Clustering

### Definition

Clustering is the practice of grouping similar computing systems together so they appear as a single unit to the larger network. Clustering can involve servers and processing, storage, even network resources.

The main benefit comes from the combined horsepower of multiple devices working on a single function or set of functions. Rather than have 20 x86 servers operating independently, clustering combines each unit into a giant computer, at a fraction of the cost of standard big iron mainframes or supercomputers.

### Business Applications

One of the chief benefits of clustering is their ability to scale. With high-speed interconnects like Infiniband, clusters can scale both resources and [I/O bandwidth](#) to meet a wide variety of data loads.

When combined with virtualization technology, clustering also supports [server and storage consolidation](#) efforts, particularly those that run extremely large databases.

Clustering also protects against failure. Modern server management systems can provide [automated failover](#) that shifts data loads to other members of the cluster should one or more devices fail.

### Deployment Concerns

As with any complex computing environment, [solid management](#) is key. Clustered systems usually involve numerous nodes and pathways, with each device maintaining a specific address and other descriptors. A central management stack is needed to keep tabs on all of this hardware and to ensure data can be accessed and delivered to where it needs to go.

Most cluster installations are coordinated through vendors, distributors, system integrators and outside consultants. Rare is the deployment that doesn't encounter its fair share of bugs, failures and integration issues.

Usually, the first step in setting up a cluster is finding an [experienced consultant](#).

## **Technical details**

A wide range of cluster software is readily available, from communications libraries like MPI to platform-specific systems like [Beowulf](#) and MPICH for GNU/Linux and [Windows Compute Cluster Server](#) for Microsoft.

Sun Microsystems recently opened up its [Solaris cluster code](#) as a means to broaden support for its overall enterprise platform.

## **COBIT**

### **Definition**

Created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI), the Control Objectives for Information and related Technology ([COBIT](#)) is a framework of best practices for IT management and governance. COBIT offers a set of approved processes, indicators, and measures to assist IT managers and users in developing an efficient and beneficial IT organization within a company. The framework has had four major releases; the latest, version 4.1, was released in May 2007.

### **Business applications**

COBIT is an important tool for business managers and auditors in the [day-to-day IT dealings within a company](#) because its control objectives help everyone—from managers down to the users—better understand the IT systems that are in use. COBIT 4.1 provides 34 processes with 210 control objectives that fit within four categories: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring and Evaluation.

Within these categories, IT managers can gain insights into decision making and IT planning. COBIT also provides guidelines for IT architecture strategies, system performance monitoring, and hardware and software planning. Auditors also find that it helps substantiate their audit reports.

### **Concerns**

Since its release, COBIT has become the globally accepted framework for IT governance and control. However, it does not compete with the Code of Practice for Information Security Management (ISO/IEC 17799:2005). Companies subject to compliance with the Sarbanes-Oxley Act would benefit from adopting the COBIT framework to help meet compliance expectations.

## Technical details

The [COBIT product package](#) is broken up into six areas: Executive Summary, Framework, Control Objectives, Management Guidelines, Implementation Guide, and IT Assurance Guide. Its structure covers four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

## Commodity Servers

### Definition

Commodity servers are servers built from [standardized components](#) rather than specialty equipment designed for a specific purpose or vendor. It is essentially the continuation of the [PC-compatible](#) trend of the 1980s, in which standard, interchangeable hardware provided the environment for the proprietary DOS and Windows operating systems.

To be a commodity, servers and their components need to share basic underlying technologies, such as a [common instruction set](#) and standard memory, I/O and expansion slot architectures.

### Business Applications

Because of the steadily increasing capabilities of modern [microprocessors](#), commodity servers have all but eliminated specialized, boutique platforms in the datacenter. Such systems still find use in [high-power computing \(HPC\)](#) environments at research labs and universities, but the lower cost and greater flexibility of commodity hardware makes it the preferred solution for most organizations.

Commodity servers are also in great demand for computer clustered applications, as advanced in networking like [10 GbE](#) and [20 G Infiniband](#) allow numerous servers to be grouped together to harness their collective processing power.

### Deployment Concerns

The major concern with commodity servers is that they are so cheap, so flexible and add so much value to datacenter infrastructure. This is turn led to widespread deployment and all of the power, cooling and cabling issues that are just now being addressed with [virtualization](#) and [server consolidation](#).

An overabundance of servers can also wreak havoc on [storage area networks](#) unless adequate investments are made to scale the two architectures in tandem. Too many requests on too few disk drives hamper response times and increases [application latency](#).

## Technical details

Despite their universal nature, the component make-up of commodity servers continues to change. The latest designs include things like an [ATX motherboard footprint](#), built-in CD-ROM and hard drive interfaces, [PCI expansion slots](#) and [Ethernet](#), [USB](#) and other connectivity features.

Many servers are also coming out with format-specific interfaces for [iSCSI](#), [Fibre Channel](#) and [FireWire](#) networking.

## Compliance Costs

### Definition

[Compliance costs](#) are defined as the amount of money and time required to meet government instituted legislations or regulations. For example, the Health Insurance Portability and Accountability Act (HIPAA) required healthcare related businesses to conform to specific data security and privacy standards. To meet these requirements, companies had to add staff, computer systems, and software, and also increase storage capacities, all of which had a major impact on budgets.

### Business applications

Depending on the specific legislation or regulation, a company may have months or years to bring itself into compliance. In the [HIPAA example](#), businesses affected had up to 24 months to comply with the final rules. To meet such requirements, a company would need to institute a plan on how to meet the objectives and decide if new staff would need to be hired or whether current staff could be trained to take on new roles or had time to perform new duties. Adding employees or training current ones for new duties can both be costly endeavors.

Other costs incurred in HIPAA compliance would include additional computer systems and software, increased paper work and paper usage, and the need for larger data storage systems. These additional costs weighed heavily on the budgets of many businesses.

### Concerns

If a business does not meet compliance standards, it would face civil and criminal fines. [HIPAA non-compliance](#) could have saddled a company with \$25,000 in civil fines per violation. Criminal fines ranged from \$50,000 to \$250,000 and imprisonment.

### Details

When such legislations are handed down, there are often [consultants](#) who specialize in bringing businesses within the compliance standards. If a company decides to attempt to meet the compliance regulations by itself, it should be sure to create a detailed compliance checklist.

## Compliance Software Packages

### Definition

[Compliance software packages](#) are groupings of software solutions created specifically to help companies meet government mandated compliance regulations. Having such a software package can help the business meet the regulatory specifications in a timely, efficient manner.

### Business applications

Once the government passes a new bill or law that sets new standards for a specific business, a company might have only a few months or years to bring itself into compliance. If the company doesn't have its own development team, it may be more cost effective to [purchase software packages](#) that are created and designed to meet the specific standards. Alternatively, a business could hire a development company that specializes in creating such software to create a customized solution just for its specific needs that also brings the business into compliance.

### Concerns

When a company is attempting to bring itself into compliance with government regulations, one of the largest concerns is always cost. Having to create (or update) current software to meet new standards is expensive when you consider it requires development, testing, training, and installation.

Other issues companies might have would be getting new software installed, up and running, and in use by employees within the timeframe instituted by the compliance standards.

### Technical details

There are many development companies that specialize in creating compliance software to meet various regulated standards including Sarbanes Oxley, HIPAA and Payment Card Industry. Some [development firms](#) will also develop software packages for a group who all need the same applications. A company needing compliance software should do its research and make sure the software they choose is from a reputable firm and that it meets all of its needs while bringing the company up to date with compliance standards.

## Configuration Management

### Definition



Network configuration management is important when it comes to maintaining robust network services with fewer data centers.

## **Business Applications**

Networks are becoming more diverse with new types of network equipment, such as WAN optimizers that join traditional routers and switches. The only way organizations can be assured that their network infrastructure is configured to deliver the required volume and quality of traffic in and out of their data centers is by fitting all of these elements in a consolidated and automated management system.

Some of the key elements of an effective configuration-management system require first and foremost an easy-to-use common interface for managing device types from different vendors.

## **Security Issues**

[Mae Kowalke](#), TMCnet Senior Editor, wrote in 2008 that IT departments at enterprises often are kept busy with the time-consuming but necessary tasks associated with changing and configuring various network devices. Such maintenance might seem mundane, but it's necessary to ensure that systems are kept running and security isn't compromised.

She notes that change and configuration management can be a problem. NSolutions with its configuration product, Network Ontology and Virtualization Appliance (NOVA), controls changes to ensure uptime and security.

## **Technical Details**

Because of idiosyncratic interfaces and command structures, it's never been easy to define, implement and maintain consistent configuration standards for the myriad of devices and vendors that populate enterprise networks. Effective network configuration management requires first and foremost an easy-to-use common interface for managing device types from different vendors. (See [The Importance of Wide Area Network Configuration](#).)

## **Content Filtering**

### **Definition**

Content filtering is the analysis of e-mail and Web content to determine whether incoming data is harmful to the network or outgoing data includes intellectual property. Such data is then blocked from entering or leaving the network to protect the business from data loss and damage.

### **Business applications**

Businesses deploy content-filtering technology for a [variety of reasons](#). Traditionally, businesses sought to increase employee productivity and preserve network bandwidth by blocking recreational Web sites such as sports and online auction sites. While that's still a benefit of

content filtering, businesses have also found the technology useful for helping to prevent malware and spam from entering the network via e-mail and Web downloads. Its most recent recognized value is in [supporting regulatory compliance](#) efforts. Regulations such as the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act put tighter restraints on the information that can leave an organization. Content-filtering technology can help prevent that information from going out in e-mails as body content or attachments.

## **Deployment Concerns**

Content filtering is often considered an enterprise-grade technology because it usually comes in the form of a pricey network-based appliance. But SMBs can turn to vendors such as Websense, SurfControl, Webwasher and Barracuda for offline content filtering.

Businesses also make the mistake of dedicating the majority of their content-filtering efforts to e-mail. However, as organizations have mitigated the threats that come in through e-mail, hackers have shifted their focus to the Web. Phishing attacks and Web downloads harboring malicious code pose as much, if not more, of a threat than e-mail viruses. Sensitive information can also leave the organization through Web mail that would otherwise go unfiltered. Experts advise businesses to focus about half their content-filtering efforts on e-mail and the other half on filtering Web content.

## **Technical details**

Content-filtering technology often uses a combination of techniques for identifying content that should be blocked. These techniques may include:

- Analyzing the header and content of incoming e-mail messages in Bayesian filtering.
- Blocking specific files, such as executable code, that attempt to enter the network as e-mail attachments.
- Analyzing e-mail headers.
- Analyzing HTML code for anomalies.
- Analyzing the content of e-mail and Web pages for inappropriate language.
- Blocking specific URLs.
- Analyzing the proximity of suspect words and phrases within content.

## **Cooling Systems**

### **Definition**

Cooling in the datacenter generally refers to two types of system: the [HVAC](#) units that keep the ambient air from overheating, and specialized [water- and air-cooling systems](#) that feed directly into server and storage racks and even to the processor cores themselves.

Heat is the enemy in complex computing environments in that it causes the [silicon pathways](#) on CPUs to break down, causing hardware failures that could result in loss of applications or, even worse, critical data.

## Business Applications

Datacenter cooling took center stage in 2007 and 2008 as the [cost of energy started to climb](#). It takes a lot of energy to cool large rooms of always-on computing equipment, so any means to reduce the heat generated by IT equipment started to see high demand. [Low-power processing](#), storage and networking equipment offered a two-pronged benefit to the data center in that they drew less power to function and generated less heat that had to be dissipated.

Efforts to [improve cooling efficiency](#) have run the gamut from installing newer energy-efficient technology to wholesale reconstruction of the data center. Raised flooring, [hot aisle/cold aisle rack configurations](#) and new chiller technologies are some of the more common steps being taken. Some firms have taken to relocating their centers to low-humidity areas like [Salt Lake City](#) and using natural rainwater and wind patterns for energy-free cooling resources.

## Deployment Concerns

Air-cooled systems are by far the more popular due to the risk of leakage in water-cooled technology, although this may start to change due to water's greater efficiency and its ability to bring the cooling element (water) [directly to where it's needed](#), much like the cooling system on a car.

Effective air-cooling often requires HVAC specialists and sophisticated software to analyze [air-flow patterns](#) in a given room and make suggestions on placement of cooling elements and room layouts.

## Technical details

Heating and cooling bring in a number of technologies that most IT staff may not be familiar with. Terms like [delta-T](#), [thermal design metric](#) and [average CPU power](#) are quickly being adding to the datacenter lexicon.

There are also organizations like the [U.S. Green Building Council](#) and [The Green Grid](#) that are working toward green datacenter standards.

## Customer Relationship Management

### Definition

Customer Relationship Management (CRM) refers to methods and technologies that help companies manage interactions with customers in an organized fashion. Increasingly, CRM relies on software (whether on the desktop, on demand, or via the cloud) to build and nurture these relationships. The ultimate goal of a CRM strategy is to identify, acquire and retain new customers or clients through the alignment and coordination of management, marketing, sales and service initiatives.

## **Business application**

CRM solutions have been demonstrated to help increase customer satisfaction, reduce operating costs and improve information sharing across the organization. According to [CRM Solutions Guide](#), companies such as Siebel, [Salesforce.com](#), PeopleSoft and Oracle have developed and implemented CRM solutions for Alta Resources, IBM, America Online and Blue Cross Blue Shield.

Among CRM providers, [SaaS](#) company Salesforce.com leads the pack, both in terms of market share and visibility to clients and competitors. The company offers modular CRM solutions for sales and service, including tools for managing marketing and leads; accounts and contacts; opportunities and quotes; e-mail and productivity; and analytics and forecasting, among others. The Chatter solution provides real-time communication between clients and sales staff to bring Facebook-like immediacy to those interactions.

Mobile CRM solutions grow in importance to businesses as IT professionals increasingly turn to smartphones, tablets and other mobile computing devices to get work done outside of the traditional office setting. Many CRM providers have already created software that works on mobile devices like Apple's iPad, according to Barney Neal of SearchCRM.com.

## **Concerns**

CRM adoption and workflow integration have been slow in the enterprise. According to a report by Gartner in 2003, companies spent nearly \$1 billion on CRM software that employees weren't using. [Jim Dickie of CSO Insights](#) offers these recommendations to increase employee adoption:

- Pick a user-friendly CRM solution; some are easier to use than others
- Select a solution based on the functionality you need; functions that aren't efficient or effective don't provide employee incentive to use the system
- Provide adequate training for users
- Provide technical support for users after training

Implementing CRM tools and services can be very complex, especially in large organizations. Therefore, detailed plans are a necessity when choosing and putting a system in place. Care should be taken to avoid fragmented implementations where CRM strategies are employed in only part of a company. This results in information silos, wherein one part or department of the company locks up information that could be of benefit across the organization. This lack of integration with the overall business strategy creates a flawed implementation that presents an incomplete view of the client that can harm customer satisfaction.

## **Data Archiving**

### **Definition**

Data archiving refers to the act of [storing digital information for later retrieval](#). Often, such data must be archived in ways that comply with strict government regulations so that information will be stored for a specific length of time and can be retrieved as easily as it was stored.

## **Business applications**

The [solution to data archiving problems](#) is not an easy one for most businesses dealing with government compliance issues for Sarbanes-Oxley, HIPAA and the Payment Card Industry. Many vendors offer their own products and platforms to help you store your data and even retrieve it. Some will even “host” your data in their own data centers.

Companies tied to government regulations must [spend large amounts of money to meet and stay within compliance standards](#), which often stipulate how long the data must be retained, how quickly it must be able to be retrieved, where the data can be stored, and in what format the retrieved data should be presented.

## **Concerns**

There are often legal concerns that go along with data archiving and government compliance. If a company’s data storage does not meet the compliance standards, severe fines could be imposed.

Companies are also concerned with costs for implementing data storage solutions, as well as the costs incurred from the need for long-term data archiving.

## **Technical details**

Many large IT-based companies offer cost-effective, reliable, [compliant and secure data archiving solutions](#) for small- to medium businesses and even large enterprises. Some provide online access, scalability, disk storage, online storage and even solutions that can [increase application performance](#) by archiving inactive data from a database.

## **Data Loss Prevention**

### **Definition**

[Data loss prevention](#) (DLP) is used in reference to computer security systems that can monitor and protect electronic data as it is used, when it travels across a network, and when it sits in a storage server. [DLP systems](#) use deep content inspection to inspect the data, detect any unauthorized use, and prevent the transmission of sensitive information.

### **Business applications**

Almost all businesses process some sort of [sensitive data that should not be viewed](#) by sources outside of the company. In the case of healthcare companies, companies that deal with credit card transactions, and even law firms, there are many government policies and regulations that

dictate how data must be secured. A company's financial data is even subject to Sarbanes-Oxley data compliance standards.

For businesses, DLP is not just a good idea; it's a requirement, often by law. To comply with regulations, or just to ensure that business data is secure, there are two types of DLP systems: network-based and host-based. There are many [DLP vendors](#) who offer such systems to help contain and protect confidential company data.

## Concerns

Besides the actual fear of data loss itself, government regulations are probably the largest concerns when a company considers options for DLP. In addition to government-mandated requirements, [many states have passed laws](#) concerning notification of customers if their data has been breached.

## Technical details

Network-based DLP involve the use of dedicated hardware and software systems, which are usually connected directly on the network. The systems work by analyzing all network traffic and identifying any unauthorized data transmissions.

Host-based DLP systems are used on individual workstations or servers. Such systems can control the flow of information between groups of users, and some can even help block users from sending out confidential data.

## Data Warehouse

### Definition

A data warehouse is a specialized [database](#) that is optimized for analysis, reporting and decision support at both the tactical and strategic levels. Data warehouses make sense because the data in production systems – such as [ERP systems](#) – is stored and managed in ways that make analysis difficult. Creating new reports is therefore a time-consuming process that requires highly trained programmers who know how and where to access the required data. In contrast, with a data warehouse the process of creating new reports is relatively quick and easy, and can be done by department-level users with no need to involve the IT department. Sometimes the content of a data warehouse is partitioned by function into department-specific databases, often referred to as “[data marts](#).”

### Business Applications

The goal of a data warehouse is better business decisions through better [business intelligence](#). Data warehouses can support this goal by providing reports that are more targeted to specific problems (Which suppliers should we eliminate?), more comprehensive (What are the effects of advertising on consumer take-away, warehouse capacity and factory production?), and available sooner – because they can be created “locally,” often by end-users themselves.

## Controversies

Vendors of production systems, notably ERP systems, argue that data warehouses are unnecessary, and that their own “bolt-on” [business intelligence products](#) are adequate or even superior. Data warehousing projects are expensive, often running into the mid-six figures, and their value is difficult to quantify because most of the benefits are indirect. Populating a database with data is complex and fraught with both technical and political problems, e.g. [who owns the data?](#)

## Technical Details

Data warehousing projects require companies to address the problem of [inconsistent data](#). This challenge, which is non-trivial, can be met via a combination of cleansing and [ETL](#) (Extract, Transform and Load). The cleansing process relates to problems with the actual data (e.g. the same individual or part listed by two different names). ETL is the process by which data is extracted from the production database, re-formatted to meet the data warehouse's requirements, and then loaded.

## Desktop Management

### Definition

Desktop management is a comprehensive approach to managing all the computers associated with an organization, including desktop, laptop and other computing devices. Also, falling under the general topic are more current enterprise concerns, such as, virtual platforms. Virtual platforms promise to rise in the IT consciousness in 2009 with widespread deployment in 2010.

Among the responsibilities within desktop management are the following: installing and maintaining hardware and software; virus protection and spam filtering; patch management for all installed applications; and administering user permissions. Desktop management tasks can be performed onsite or via the Internet with a remote support solution. See [On Top of Virtual Desktop Management](#) for further insights.

## Business Applications

The technology is ready to provide seamless connectivity with little or no application latency. Desktop virtualization solutions generally break into two types: server-based and client-based. Server-based virtual desktop models are most appropriate for fixed PCs that have constant LAN network connectivity to a centralized server farm where computation takes place. This approach can work over the WAN for certain applications, but latency and mobility are challenges, especially for the 50 percent of PCs that are laptops.



Client-based desktop virtualization is most appropriate for organizations that have laptops and remote users; in this model, virtual desktops run locally on the end-user PC, with centralized management and policy enforcement. Kidaro's platform uses client-hosted desktop virtualization, which has the benefits of supporting fixed users, mobile users, and disconnected use in a single infrastructure, while avoiding the need for expensive server farms. (See [On Top of Virtual Desktop Management](#).)

## Security Issues

Desktop virtualization can help enterprises realize dramatic improvements in security but only if it is integrated into existing infrastructure and processes. Security is merely one aspect among many for desktop-management solutions. It is best to build it in when creating the entire process, that is, when addressing distribution, integration, formatting, and so on. Plus, security is a potentially paramount management headache with laptops and other unmanaged computers.

## Technical Details

Many organizations would like to provision enterprise access to consultant laptops or home PCs, instead of buying laptops for these users, but they're concerned about inviting unwanted malware and vulnerabilities onto their network. Kidaro enables enterprises to deliver a "virtual laptop"—essentially an encrypted, corporate-managed virtual machine that can run off a USB drive or be downloaded over the Web onto any PC. This allows organizations to provision access rapidly to new users, consultants, home PCs or M&A scenarios without worrying about the underlying operating system or configurations.

## Disaster Recovery

### Definition

Disaster recovery refers to a set of [backup, recovery and related systems and processes](#) designed to get a data center up and running in case of a major failure.

The popular impression is that disaster recovery is only used for major events like earthquakes or explosions, but [serious outages can occur for a number of varied reasons](#), including technology failures and human error.

### Business Applications

The main goal is to get [critical systems](#) up and running as quickly as possible. To that end, enterprises have deployed a number of technologies to ensure a quick response. Among them are [data mirroring](#), [remote storage](#), [hosted applications](#) and [virtualization](#).

An increasingly popular strategy is the deployment of [thin client architectures and virtual desktops](#) that essentially allow workers to tap into business applications wherever they can. But even this approach relies on rapid availability of organization data either from a central or remote location.

## Deployment Concerns

As with any storage and recovery issue, [security](#) is a key concern. During a major failure, systems need to be responsive to requests that may or may not be coming through standard network channels. Ensuring that these requests are valid in a timely manner can prove to be a significant challenge.

Another concern is the habit of [ignoring disaster recovery systems](#) and requirements until they are needed. Organizations that have experienced critical disruptions say DR needs to be an ongoing process in which systems are routinely tested and users are familiar with the processes and procedures to get back on-line.

Disaster recovery is also viewed by some as a major cost center with only a remote chance of ever being used. That view tends to suffer when news breaks of a major outage somewhere in the IT universe.

## Technical details

DR entails a number of key technologies such as [business continuity software](#), [disk- or tape-based archiving solutions](#), [data protection](#) and [replication](#) and mirroring technologies.

DR planners also become familiar with terms like [recovery point objective](#) and [recovery time objective](#), which are used to gauge the effectiveness of plans to bring enterprise platforms back into operation.

Restoration of [power systems](#) is also critical, requiring redundancy in devices like uninterruptible power supplies, surge protectors and the like.

## Digital Rights Management

### Definition

[Digital rights management](#) (DRM) refers to the effort by publishers and copyright holders to provide copyright protection for digital media, usually via various technologies that limit or control access to the media. [These technologies](#) were first developed after the onslaught of peer-to-peer file exchange programs (i.e. Napster) that were used to pirate MP3 music files and video files across the Internet.

### Business applications

In the work place, you might run into such DRM technologies as the Output Protection Management (OPM) on [Microsoft Vista](#). Within this system is the Protected Video Path (PVP), which keeps the computer from playing restricted content. PVP also limits the PC from making unauthorized recordings.

### Concerns

Although copyright holders do need to protect their work in order to make a profit, [many users contend](#) that the technologies currently developed for DRM actually restrict use of the media too much. There is also worry that [DRM restrictions will not expire](#) even after the copyright on the media has expired.

### **Further information**

There are many ways to bypass the DRM control technologies, which make the use of DRM a bit, well, useless. There are [software programs](#) that help decrypt restricted files, watermarks can be removed from images and film, and CDs and DVDs can be copied and traded without much restriction.

## **Document Management**

### **Definition**

Document management involves the organization, filing, storing, retrieving, and archiving of documents—both digital and paper--created by a company. There are many ways a business can manage its documents, from a filing cabinet to a sophisticated content management system.

### **Business applications**

Most businesses create hundreds to thousands of documents each year that must be filed and saved for later use. If the company deals with document creation on a daily basis, a digital document management system would probably be cost-effective for daily usage and long-term storage and retrieval. However, if it is a small business dealing with a very few paper documents, it may only require one person to safely organize and file away documents.

To create a [method for document management](#), a company should ensure that the system addresses the following points:

- The location of the document storage
- How the documents will be filed
- How will documents be retrieved when needed
- What methods of security will be enforced
- How can the documents be recovered after a disaster
- How long the documents should be retained
- How to keep the documents in a format that ensures future readability
- How documents will be made available for those who must use them
- A set of rules to allow workflow among employees who deal with the documents
- Rules for document creation and version control
- Ways to ensure authenticity of the documents

### **Concerns**

There are many issues that cause concern when a company considers document management. Obvious concerns include version control, security, and recovery after a disaster. With digital document management, you must also consider archiving issues, i.e. will the documents created and stored today be in a format that is readable in the future?

For law firms, the [Federal Rules of Civil Procedures](#) govern the retention of documents from civil cases, so there are government compliance issues that must also be considered. Also, the U.S. congress passed a bill that calls for [digitizing all health records](#) for its citizens, so businesses that deal with healthcare issues will need to comply with those standards.

## **Technical details**

[Digital document management systems](#) allow for collaboration, convenient workflow, version control, integration into various applications, tracking of documents as they flow through the system, and retrieval and publication options. There are many companies that provide document management systems, and choosing such a system will depend greatly upon the type and number of documents a business must create and manage, as well as the systems with which the document management system must work.

## **eDiscovery**

### **Definition**

Electronic discovery, or [e-discovery](#), refers to “discovery” as it is traditionally used in litigation and “electronic” as in digitally stored data, such as instant messages, e-mail, and any other files created and stored digitally that may be of relevance in a legal case. When used in terms of litigation, “discovery” refers to the process by which both sides of the case attempt to uncover all relevant information about the suit by requesting documentation from the other side.

### **Business applications**

In December of 2006, amendments to the [Federal Rules of Civil Procedures](#) were passed to include processes and guidance for e-discovery. Basically, [e-discovery](#) includes any digitally created documents or information.

Any business could end up in [litigation](#) at any time. This is why it is important to have a good data management and document archiving system, and a good relationship between the IT department and the legal department. Once pertinent documents are requested, a company must be able to locate and retrieve the necessary files quickly and easily.

### **Concerns**

A new concern in the area of e-discovery is that of [virtualization](#). When a forensic examiner is searching a user’s hard drive for relevant data, files contained on virtual machines might not

show up during the searches. If a company is involved in litigation and they use virtualized systems, it is important that they explain the type of virtualization to the attorney and any forensic investigators so that they can make sure that all pertinent documents are retrieved.

## **Technical details**

One of the more important aspects of such digital data is its metadata, which is a part of each electronic file that shows when the file was created, who created it, if it has been modified, etc. Once a file is requested for a lawsuit, forensic investigators can search through its metadata to ensure that the file is original and has not been tampered with. This is why it is also important that the files are kept in their original file format, also called a “native” format.

## **EII**

### **Definition**

Enterprise information integration products query data from various sources – hence, it's considered a “pull” technology - and gives users the information in a unified view at the presentation layer. That might be a dashboard or a report. EII tools can work with structured, unstructured and semi-structured data.

EII does not move data from its source location, although sometimes the queried information is held in a virtual database. However, some EII tools can update those sources.

EII became a hot IT topic in 2004 and 2005.

### **Business applications**

As with so many other types of integration technology, EII is used to provide business users with a “single view of the customer.” Regulatory compliance and the need for real-time business information have driven adoption of EII tools.

EII products are middleware for data services, allowing you to access multiple data sources without hard-coded integration to each source. It uses a loosely-coupled, service-oriented approach to integration, [according to this Computerworld article](#). Because of its service-oriented approach, EII can be used for some projects that would have required custom coded, point-to-point integration – a very expensive process.

EII tools can be used to present information through reports, dashboards, portals, applications and even through mobile devices.

### **Deployment concerns**

Before you invest in EII, there are steps you can take to prepare for information integration. [eBizQ recommends this list](#) of information-integration best practices for those considering EII.

You should also consider the following before investing in an EII tool:

EII products usually include a set of adapters to simplify connecting to back-end data sources, but you'll want to ensure the adapters meet your needs. You may have to either create new connectors or modify existing ones for your own situation. Determine how robust data modeling and metadata management need to be to address your needs.

Some tools allow you to interact more with the back-end data sources than others. The type of [information](#) you'll be accessing might also affect the type of adapters you'll need.

EII is not a substitute for data warehouses. EII is not useful for conversions, transformation and historical data, [according to Michael Schiff, principal consultant for MAS Strategies](#).

Another issue organizations should be aware of is EII's striking similarity to customer data integration (CDI) and master data management. [Intelligent Enterprise pointed out](#) all three are pull solutions that use metadata and a model-driven approach to integration, noting that CDI and EII in particular “are essentially the same technology, packaged differently for their respective purposes.”

## **Technical details**

Data modeling, metadata management and XML tagging are all key aspects of EII. One consideration with EII tools is support for data caching and staging to improve query performance, according to [Intelligent Enterprise](#). [Wise Geek notes](#) that EII's virtual caching of data is “perhaps the most unique feature of EII.”

For a more technical discussion of EII, check out “[Which EII Solution Is Right for You?](#),” published at Java Sys-Con in 2004.

## **Enterprise Servers**

The term “enterprise server” usually denotes a class of either [hardware- or software-based server](#) capable of handling the complex computing environment of a large enterprise.

Enterprise servers can be general processing machines that move application workloads between end-points, or they can be a specialized device such as a [web server](#), [print server](#) or [database server](#).

## **Business Applications**

The enterprise server has become the workhorse of the modern office environment, largely replacing the [big iron mainframes](#) that dominated from the 1960s to the early 1990s.

Most servers these days are built on [commodity components](#) and are capable of running all of the major server OS platforms like [Microsoft Server 2003/2008](#), [Linux](#) and [Mac OS X Server](#).

## **Deployment Concerns**

The key concern in deploying servers is reliability. Since so much valuable data is entrusted to these machines, any downtime can seriously impact performance and, ultimately, profits.

Most server infrastructures are designed with a wide range of [backup](#) and [failover](#) systems so that if one device fails, both data and resources are available elsewhere with little or no interruption for the user.

Another major issue is server sprawl, which is essentially over-deployment of servers designed to accommodate short-term data processing needs. Many firms have turned to virtualization to [consolidate the number of servers](#) in their farms to gain greater hardware utilization rates and lower capital and operating costs, particularly energy consumption, in the bargain.

## **Technical details**

Most of the technologies used to construct a server can be found in a standard workstation as well. So there is a [CPU or set of CPUs](#) embedded on a motherboard, with associated memory systems, networking components, a graphics/video card or cards and related power supply equipment.

A recent development is the [blade server](#), which provides only the most basic server components to the motherboard and shifting much of the network and power systems to an outside enclosure where they are shared among other blades.

## **Enterprise Service Bus**

### **Definition**

The term “Enterprise Service Bus” can be used to mean an architectural style, but is more widely used to refer to software that carries information between applications

### **Business applications**

ESBs are used for integrating systems and applications. ESB as a technology evolved from enterprise application integration. Rather than using point-to-point connections between applications, you can send messages or “calls” through the ESB, which routes them to the appropriate applications. In practical terms, this reduces the cost of custom coding and can make your systems more efficient.



Think of it this way: In the real world, a bus is used to eliminate the need for an individual to walk or drive from place to place. In the software world, applications do not need to have a direct connection to each other if they have access to an ESB.

But ESBs are not simply couriers, unquestionably delivering messages. They can also “translate” messages for legacy applications that do not support messaging. In simple terms, this means the ESB will put the data in a format the legacy application can use. This is done with an adapter, and most ESBs include numerous adapters.

An ESB can also be used to enforce business rules. According to a 2006 special report on ESBs published in [Visual Studio Magazine](#), an ESB can add specific services to messaging, including:

1. Security.
2. Priority-based routing.
3. Content-based routing.
4. Adapters for different types of code, which are used for communicating with legacy systems.

Finally, since ESBs generally include a repository that assists with prioritizing messages, many organizations use ESBs as a backbone for their service-oriented architecture (SOA). The services can be stored in the ESB repository. The ESB then delivers and mediates services.

ESBs are often deployed when Web services form the core of the SOA. However, it's important to remember that while many organizations have found ESBs helpful, they are not required to build a SOA. In fact, there has been some [debate](#) about whether ESBs are detrimental as a foundation for SOA.

## **Deployment Concerns**

There is disagreement in the industry about when ESBs should be used, and to what extent. For instance, while an ESB can be used to enforce business rules related to security and message priority, Chief Technologist and IT Toolbox blogger Eric Koch warns against [putting business logic in the ESB layer](#):

“I have worked on several ESB or integration broker rip-outs. Invariably developers put too much business logic into the ESB layer and do not practice fundamental architecture principles such as layering and separation of concerns. They turn the ESB into the intermediary of choice, creating a service hub. This defeats or overlaps the role of the service registry and complicates the overall architecture.”

While ESBs are common tools in enterprise architecture, not everyone is a fan. At QCon London 2008, ThoughtWorks’ chief scientist Martin Fowler and Dr. Jim Webber, global head of architecture for ThoughtWorks, [argued](#) that most enterprise-scale ESBs are so bloated, they can hinder agility. Instead, they advocate Web-centric design. Of course, their criticism of ESBs attracted [critics](#) of its own.

Others are concerned about the proliferation of ESBs. Since ESBs are used to send messages between different systems and applications, vendors have increasingly added ESB solutions to their software platforms. As a result, organizations find they're running multiple types of ESBs. [Some](#) have questioned whether this could cause problems – essentially, requiring you to integrate solutions designed to solve integration problems.

The counter-argument is that ESBs are designed for integration, so integrating multiple ESBs is easy and of little concern.

## Environmental Regulations

### Definition

An environmental regulation is any legal restriction that is enacted to control the way people interact with the environment in order to reduce the negative effects of human interaction with nature. Most of these regulations are enforced by the U.S. [Environmental Protection Agency](#) (EPA).

### Business applications

Depending on the specific regulation, there are many ways these restrictions can affect business. For example, to comply with EPA regulations, a business needs to know the [proper way to dispose of old computers](#) and electronics equipment.

### Concerns

Some have complained that environmental regulations [have gone too far](#); however, another argument reveals that perhaps they [haven't gone far enough](#). There has been a recent era of deregulation that some say has spurred along the global warming problem.

## E-mail and Web Policies

### Definition

E-mail and web policies are basically [usage policies](#) set by a company governing the proper use of company e-mail and Internet access. Some companies prefer strict work-usage only. Other companies allow employees to use work e-mail and web access for personal use.

### Business application

All companies need a set of rules to explain what is and is not acceptable in the ways of personal versus business e-mail and web use. When writing [such a policy](#), management and the IT staff should consider defining personal use, setting rules on copyrighted material and downloads, explaining issues with downloads and viruses, spelling out unacceptable use, and listing disciplinary actions that will be taken if the user does not stick to the policy.

## Concerns

As with all policies and guidelines, employees often complain about strict rules. Some may even try to find ways around certain parts of the policy. Be sure that the [policy is enforced consistently](#), though. Being lax about rules might open up your network to viruses, porn, or other unacceptable usage.

## Technical details

There are several sites that provide [sample e-mail and web use policies](#). There are also companies who provide products for monitoring employee [e-mail](#) and [Internet use](#).

## E-mail Security

### Definition

E-mail security refers to the measures used to protect e-mail systems against a multitude of threats, including malicious code and data loss. There is a breadth of hardware, software and procedural methods that support e-mail security, and they are often used together to help ensure optimal protection.

### Business applications

E-mail is a popular attack route for those attempting to steal sensitive information or disrupt business operations. E-mail also is considered a mission-critical application for many businesses, so its availability and integrity is of utmost importance. Businesses that neglect e-mail security are putting their companies at great risk.

Businesses can choose to deploy their own technologies as part of their e-mail security, or they can choose to outsource e-mail security to a service provider that filters incoming e-mail for malware, spam and other objectionable content.

### Deployment Concerns

Businesses should be careful not to [oversimplify e-mail security](#). Desktop antivirus alone will not protect systems. Not only does e-mail face a variety of threats due to its very nature, it is also used differently by users and whole departments within an organization. Thus, implementing an e-mail security policy and the technology to support it can be challenging. Some users may be using e-mail as a filing system that, as a result, holds sensitive data, while departments may have varying levels of tolerance for e-mails that could pass as spam. Businesses should be sure to involve representatives from different departments to help ensure that all business needs are met while addressing otherwise hidden security vulnerabilities.

Of course businesses also have to keep up with e-mail security technologies. According to a survey by IDC, [72 percent of companies are unable to stop data leaks via e-mail](#) and 9 out of 10 companies do not have effective spam filters in place. New e-mail security solutions come on

the heels of new threats. Businesses must keep their technology updated to remain protected against the latest threats, whether that means updating threat signatures or replacing hardware altogether.

Businesses interested in [outsourcing their e-mail security](#) should consider who will be controlling a critical piece of infrastructure. The business no longer has control over the e-mail systems when they are outsourced. For this reason, it's especially important that businesses consider the e-mail security strategy adopted by the service provider, who is just as vulnerable to e-mail security threats as its customers. Businesses might also consider the potential delays that might result from adding one more "hop" in the e-mail route. Although many service providers have mitigated this concern by building a fully redundant infrastructure that is load-balanced across multiple data centers.

### **Technical details**

E-mail security appliances are an all-in-one approach to e-mail security. These hardware devices sit on the network, near the firewall. Incoming and outgoing e-mail is intercepted by the appliance, which scans messages for malware, spam and sensitive data. Some e-mail security appliances offer advanced features, and can also be configured to enforce security policies and regulatory compliance requirements.

A variety of software is also available to support e-mail security efforts, including encryption, antivirus, content filtering, anti-spam, anti-spyware and security suites, which package different software together into a single application.

Other network security technologies such as routers, intrusion-detection systems, and content filters can also support e-mail security efforts.

## **E-mail Servers**

### **Definition**

As the name implies an e-mail server is a hardware system that specializes in the transfer of e-mail from one device to another.

An e-mail server usually encompasses a software program known as a [mail or message transfer agent \(MTA\)](#) that contains the protocols and coding needed to keep [domain names](#) and [IP addresses](#) organized and accessible.

### **Business Applications**

E-mail is now such a crucial component of modern life that it has become indispensable to businesses and virtually any other human organization.

A properly functioning e-mail system generally receives a great deal of support, both capital and operational, particularly since the rise of [mobile computing](#) and e-mail enabled mobile devices like cell phones and [PDAs](#).

## **Deployment Concerns**

With the growing presence of multi-vendor and multi-platform enterprises, assuring that a single e-mail system can operate under all environments is a big challenge. OS support may not extend across Windows, Linux and Mac OS X, for example, and not all servers will support both database and [filesystem](#) storage. This doesn't necessarily mean that mail won't get delivered, but adds to engineering and infrastructure costs to ensure the entire enterprise has access to a common feature set.

Different e-mail systems may have varying types of [authentication features](#), [anti-spam tools](#) and other capabilities as well, making some organizations or parts of organizations more susceptible to disruptions than others.

[Integrating disparate e-mail systems](#) is usually one of the most difficult and time-consuming IT jobs following a merger or acquisition.

## **Technical details**

The leading e-mail server platforms include [sendmail](#), [Microsoft Exchange Server](#), [Postfix](#) and [Exim](#), although the rise of hosted e-mail services like [Postini](#) (now part of Google) is starting to eat into that market share.

Besides the MTA, an e-mail server will usually contain subsystems like a [mail exchanger](#) to organize user addresses, a [mail user agent \(MUA\)](#) that provides the user interface and associated [mail delivery agents \(MDAs\)](#) to facilitate that actual message delivery.

E-mail servers also include a wide variety of tools to address [archiving](#), [web administration](#), [traffic control](#), proxy connections, search and a host of other functions.

## **ETL**

### **Definition**

ETL is short for extract, transform and load. ETL extracts data from one or more data sources, transforms the data from its previous form into a form usable by the target database or datawarehouse, and finally, loads the data into that target location.

### **Business Applications**

Traditionally, ETL is widely known as a tool for moving data from multiple databases to a data warehouse. However, in 2008, Bloor Research Director Philip Howard [cited](#) research showing there are four use cases for ETL tools:

1. Data migrations and conversions, which, with data warehousing, compose two-thirds of all ETL projects.
2. Application synchronizations, such as moving data from an ERP to a CRM system.
3. Business-to-business exchanges for converting SWIFT, HIPAA and other messages.
4. Providing data services for service-oriented architectures.

In addition, ETL tools generally also can [perform data cleansing](#). ETL is typically a tactical deployment, but it can be used strategically, as evidenced by this case study of a solution developed by IPS-Sendero, a software-development company and professional services company that focuses on [corporate performance management](#).

## Deployment Consideration

Ralph Kimball, founder of the Kimball Group and author of "The Data Warehouse ETL Toolkit," noted that while ETL stands for three steps, the best practice for ETL systems in most data warehouses actually requires 34 subsystems, which he categories into [four major components](#): extracting, cleaning and conforming, delivering and managing.

The point is, ETL is not as simple as it may seem. While you can buy ETL tools, expect to spend some time addressing issues of data quality.

Also, ETL solutions may sound similar on paper, but in practice, they perform differently, so it's advisable to identify your technical criteria and test products against these before you invest. Here are some questions to consider:

1. Do you need support for Web services?
2. Do you need an XML-based tool?
3. How scalable must the tool be?
4. Will you need to repurpose the tool within the organization? If so, what is the cost per project?
5. Will you be embedding the ETL engine and distributing it?
6. Can you do a trial run? Most ETL the tools are too complex for a proof-of-concept, but some companies do offer short-term licenses for single projects.
7. How does the tool perform? Does it run the required transactions at the speed you need?
8. What will the total cost of ownership be?

## Emerging Changes to ETL

While ETL remains a standby, some companies are replacing ETL with newer, alternative integration tools. Pfizer Global Research and Development deployed data-integration middleware to eliminate ETL projects. As a result, research and development teams were [able to](#)

[gain access to data](#) within a week, rather than the three- to four-month timeline required by IT to run new ETL jobs.

For the most part, however, traditional ETL vendors face competition from next-generation ETL tools, such as expressor, which uses a [semantic metadata repository](#). These new competitors, and established vendors' response, are explored in this Enterprise Systems [article](#).

[Some](#) predict master data management might also emerge as a competing solution to ETL.

## External and Internal Audits

### Definition

[External audits](#) occur when an outside auditor is hired to come into a company and review its books. An external audit presents an entirely unbiased review of an organization or company's financial statements.

An [internal audit](#) involves an auditor analyzing business processes, reviewing operational procedures, or even measuring how well a company complies with standards and regulations. After an internal audit, problems and issues are highlighted and solutions and fixes are recommended.

### Business applications

Both types of audits are important to businesses, especially those that are publicly traded, are part of a government agency, or are otherwise relied upon by the public.

An external auditor wants to ensure that a company's financial information is in line and that it gives a true representation of the company's financial situation. Since the passing of the Sarbanes Oxley Act, external auditors have strict guidelines on their evaluations on publicly traded companies.

Internal audits are primarily to make appraisals of a company or organization's practices and processes, including risk management, IT, and any governance issues.

### Concerns

In the [internal audit](#) arena, studies have shown that some auditors spend too much time addressing risk management processes and not enough time reviewing and addressing actual business and operational risks. Other studies have shown that companies are spending less of their budgets on internal audits, instead choosing to focus on external, financial audits.

The Sarbanes-Oxley Act may have companies focusing attention on external audits, but the problems may exist with the actual auditors. The Public Company Accounting Oversight Board reported that even the top eight firms have exhibited weaknesses and oversights in their audits.

## Firewall

### Definition

A firewall is a system consisting of hardware, software or both designed to prevent unauthorized traffic from entering a private network. The [firewall examines all packets](#) to determine whether they should be allowed through based on pre-defined policies.

### Business applications

Network firewalls have long been considered a necessary component of a network security strategy. They are most commonly implemented at the network gateway to prevent unauthorized traffic from the public Internet from entering the private intranet. However, they can also be implemented between network segments to enforce varying levels of trust. You might, for example, choose to filter traffic coming into the sales department's portion of the network to ensure that users from other departments are not accessing sales-related resources.

### Deployment Concerns

As the network's first line of defense, a network firewall is inarguably important. But an organization's security efforts should not stop there. There are many [threats that a firewall cannot stop](#), including distributed denial-of-service attacks, spam and data leakage. Even though firewall manufacturers are continually [updating their technology](#) to keep up with the barrage of threats, experts strongly recommend implementing a [layered defense](#) that includes antivirus, intrusion detection and content filtering.

Also, a network firewall is only as good as the policies it enforces. Best practices advise implementing "default-deny" rules in which the firewall denies all network connections by default unless a connection is specifically allowed. However, given the number of endpoints and applications accessing the network on a daily basis, it is much more practical – and therefore more common – for organizations to implement "default-allow" rules. In this case, all network connections are allowed unless explicitly denied or blocked.

### Technical details

[Firewalls can filter traffic a number of ways](#) and may incorporate multiple methods. In addition to packet filtering in which the firewall inspects individual packets attempting to enter the network, a firewall might serve as a proxy, executing requests on behalf of internal users. This frees users from connecting directly to the Internet. Bastion hosts, on the other hand, intercept all network connections coming from the Internet. Some firewalls also use network address translation, which helps organizations conserve the number of IP addresses they need while protecting sensitive hosts by changing public-facing IP addresses.



## Firewall Internet Security

### Firewalls

Enterprise companies today employ firewalls that do careful inspection of sessions between external and internal hosts and devices. Cisco employs a patented ASA algorithm that utilizes source IP address, destination IP address, TCP sequence numbers, port numbers and TCP flags to examine and prevent unauthorized sessions. The firewall is configured with conduit

statements to filter traffic by examining source/destination IP addresses, application port and protocol port before making a decision whether to permit or deny a session or specific traffic.

Firewalls are implemented at the company demilitarized zone (DMZ) which is located between the external network and the company internal network. Static routing is typically configured at the DMZ between firewalls and internal/external routers for improved security. This is to have greater control over route propagation than would be available with dynamic routing protocols such as RIP and EIGRP. Internal and DMZ (Public) servers would be configured to use the firewall as their default route to forward Internet traffic. If an internal router were available, servers would use that as their default gateway to forward Internet traffic.

The external router broadcasts a default route to the firewall that is used to forward traffic destined for the Internet. A conduit must be configured at the firewall for each protocol type that should be allowed through your firewall. For instance, if your company manages routers and servers across a firewall, you must configure a conduit for SNMP traffic to allow traps through the firewall. The conduit would specify the source address of the router which is sending SNMP traps, the destination address of the network management station that is receiving SNMP traps, and UDP 161 which is the UDP port number for sending SNMP traffic from managed devices to a network management station.

The firewall examines the end to end session connection and does a lookup of its conduit table to determine if a particular source address, destination address, protocol port or application port is allowed through. The packet is discarded or allowed through on to the company network (inside) or Internet depending upon the conduit statements configured.

### TACACS Server

This is a TCP service running on a designated Unix server that authenticates employees attempting to access a router. The routers must be configured to send a request to the TACACS server when someone attempts to logon to a router. The router prompts the user for a username/password pair and sends that to the TACACS server for authentication. TACACS servers are implemented with VPN services as well to authenticate remote users before allowing that session to continue with network authentication to Windows Server, Unix or Mainframe authentication and authorization.

### RADIUS Server

This is a UDP service running on a designated network server that authenticates employees attempting to access a router. The routers must be configured to send a request to the RADIUS server when someone attempts to logon to a router. The router prompts the user for a username/password pair and sends that to the RADIUS server for authentication. RADIUS servers are implemented with VPN services as well to authenticate remote users before allowing that session to continue with network authentication to Windows Server, Unix or Mainframe authentication and authorization.

## Green Technology

### Definition

[Green technology](#) involves using science to create technologies that conserve natural resources and [lessen the human impact on the environment](#). At the core of green technologies is the attempt to create products and methods that are based on sustainable pieces and parts.

Many green tech products are helpful in conserving energy or reducing waste. Some also provide or use alternative energy sources, such as solar power, to help cut down the carbon footprint of the person who uses the technology, as well as the company who employs the technology.

Green technologies include such areas as renewable energy sources, waste management, remediation of environmental pollutants, sewage treatment, recycling and water purification. Many large corporations are attempting to incorporate several of these technologies along with [IT products](#) that help them conserve energy and reduce internal waste such as paper printouts.

### Business Applications

Most businesses attempt to [employ green technologies](#) to conserve energy and reduce their carbon footprint. The greening of many companies begins with the incorporation of renewable energy sources and green IT equipment. Even large companies such as [Hewlett-Packard](#) have begun using solar power to offset the amount of energy relied upon from nonrenewable sources.

Other enterprises begin their foray into green IT with the creation of a [green data center](#). Since data centers consume intense amounts of energy in comparison to a regular office, companies see a greater impact on energy reduction when they adopt greener technologies there. Creation of a truly green data center includes using green technologies within the building along with [green IT equipment within the center](#). However, companies can still begin a green initiative by using greener, more energy efficient servers and [computers](#).

### Concerns

Current concerns with green technology are that making the switch to environmentally friendly products and methods is costly. Solar panels, green building supplies, and green IT equipment all cost more than regular technologies. During this time of global economic crisis, companies have

a difficult time justifying the purchase of such technologies even if the longer-term savings can be proven. However, many companies are offering ways to [reuse systems with greener additions and optimizations](#), which can help convince management to move toward greener initiatives.

## **Green Computing**

The impact of IT and computers in general on the environment goes beyond power consumption. To truly adopt green computing ideas, a company should consider how their current computers and equipment are reused or disposed of, the purchase of replacement equipment that is both energy-efficient and created with environmentally sound parts, and the energy consumption of current systems that are in use.

Green computing can also involve the use of virtualization, terminal servers, and solid-state storage drives. Virtualization involves combining several systems onto one machine, which reduces power and cooling required to run multiple systems. There are also many companies that provide software to help businesses create their own virtualized computers.

Terminal servers provide a central server to which users connect in order to access software. When combined with the use of thin clients, a company can save up to 1/8 the energy of a typical workstation—a significant savings for many businesses.

For a company who requires a lot of data storage, solid-state drives might be the green IT solution. Such drives can save on operating costs while boosting performance speeds and reducing the company's carbon footprint.

## **HIPAA**

### **Definition**

In 1996, the U.S. passed the [Health Insurance Portability and Accountability Act](#). There are two specific areas to the act: Title I spells out regulations to preserve health insurance coverage when people lose or change their jobs, Title II sets standards for healthcare information systems. It also includes a Privacy Rule that went into effect in April of 2003.

### **Business application**

HIPAA has had the most impact on medical and healthcare related businesses. Such companies must comply with a long [list of requirements](#) including providing secure protection of medical information for all patients and clients, utilize standard formats via new programming codes, and have their new systems certified to show that they meet all the requirements spelled out in HIPAA.

### **Concerns**

In the years following the [HIPAA enactment](#), the medical research sector has taken a direct hit. Because of the strict privacy rules, [researchers](#) have been unable to do chart-based studies and follow-up patient surveys.

Also, some medical offices and doctors still do not fully understand all of the regulations and therefore are less open about disclosing information—even information that a patient may have a right to access.

There have also been concerns over the cost to completely comply with all of the regulations. Medical-based companies were required to institute new computer systems and practices within their offices, which required more money to install, train, and support. There has also been an increase in the amount of paperwork required for patients and clients, not to mention ongoing needs to [stay abreast of any changes](#) and ensure that offices remain in compliance.

## Hosting

### Definition

Hosting refers to the practice of [outsourcing enterprise applications and/or resources](#) to a third party to be delivered back to the client over a network infrastructure, usually the Internet.

The rise of [high-speed networking](#) over the past decade made it feasible for organizations to provide these services on either a fixed- or flexible-rate basis, alleviating the cost and complexity of maintaining systems and applications in-house.

One view is that many [smaller businesses will turn to the hosting model](#) for their IT needs because it provides a virtually unlimited, scalable architecture that is billed according to use.

### Business Applications

Just about any application or function provided by an in-house IT infrastructure can be duplicated by a host. Hosting organizations can deliver processing power and storage for application workloads, as well as the applications themselves.

Many of the leading organizations offer full suites of business applications, such as databases, [Business Intelligence \(BI\)](#), [the Sidekick story](#) and a host of others. Middleware management stacks and systems analysis platforms are also common.

### Deployment Concerns

Chief concerns of the hosting model center largely on the [told me before](#) and the vagaries of the public networks on which most services operate. Service interruptions can shut down business operations at hundreds of enterprise organizations at a time, leading to lost productivity and direct revenue loss.

Defenders of the model argue, however, that their services are no more prone to failure than many internal IT infrastructures.

Unlike internal [Ethernet-based infrastructures](#), however, hosted services are generally restricted to the broadband speeds of the Internet, causing many users to complain about high latency.

## Technical details

Hosting can be broken down into a number of specific implementations, such as [Software as a Service \(SaaS\)](#), [successful Dynamics AX implementation](#) or even [Everything as a Service \(EaaS\)](#).

Each of these models relies on a range of technologies like virtualization, high-speed networking, [Safety in the Cloud: 'Vaporizing the Web Application Firewall to Secure Cloud Computing](#) and others to form as robust a service as possible.

## Internal Threat

### Definition

Internal threat refers to the threat posed by the users of an organization's network and/or information systems. These users are insiders in that they are authorized, at some level, to use the organization's technological resources. However, every user poses a threat to the integrity and availability of those resources, either through malicious intent or accidental misuse.

### Business applications

The internal threat is often considered an [organization's biggest security risk](#) because users require a level of trust to carry out their day-to-day tasks. Also, organizations tend to focus on securing the network perimeter from outsiders, as opposed to securing network resources from insiders.

Experts recommend educating users about security and proper computer use to help reduce internal threat. There are also technical controls organizations can implement. Together, security-awareness training and technical controls can help prevent malicious attacks and accidental misuse of IT resources.

### Deployment concerns

There are several dynamics to the internal threat. We're not just talking about insiders sharing passwords. There's also the [full-time telecommuter versus the office worker](#); the user working around stringent policies to get her work done versus the accountant shaving a few pennies off the numbers. Then, of course, there is the [laid-off](#) IT manager who uses his access as blackmail. Organizations need to account for these many possibilities and implement appropriate risk-mitigation techniques.

## Intellectual Property

### Definitions

[Intellectual property](#) (IP) rights are defined as property rights that concern anything created by your mind, including commercial and artistic designs and ideas. The two main areas of IP are [industrial property](#) and [copyrights](#).

### Business applications

In the business world, things are created every day. For most workers, the ideas and concepts they create on the job are [owned by the company for whom they work](#). An interesting case has come about recently that challenged the creative rights—who owned the rights to the Bratz dolls. [Mattel](#), who had filed against the creator of the Bratz dolls because he had created the concept for the dolls while under their employment, ultimately won the case.

### Controversy

There are many who believe that IP rights go against the good of the public interest—especially when you consider that [copyrights can be extended](#) and patents can be placed on business methods and [software](#). Such acts offer protection to the IP owner, but at what cost to the public? How long should someone be able to hold a patent on software? Others warn that this is a form of “[intellectual monopoly](#).”

### Further details

IP rights cover a broad area of creations, which generally fall into two categories—copyrighted creations and industrial properties. Copyright laws cover photographs, software, books, music, paintings, and movies. Patents are granted for specific inventions, and this falls into the industrial properties area.

## Internet Governance

### Definition

The Internet is not owned by a single political, governmental organization. There is much disagreement over who and what is governed on the Internet. There have been attempts by many organizations to impress their ideals or laws upon this international entity. As of today, no one has been allowed to claim rights over the Internet.

A group put together after a United Nations WSIS (World Summit Information Society) proposed this definition of Internet governance on [page 4 in their June 2005 report](#): “*Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet*”

## **Business applications**

There are different bodies that control the various pieces of the Internet today. The [Internet Architecture Board](#) (IAB) gives oversight for publications from the [Internet Engineering Task Force](#) (IETF), and is an advisor to the [Internet Society](#) (ISOC). The IETF provides technical specifications and request for comment (RFC) for review and enhancement of Internet technologies. The [Internet Research Task Force](#) (IRTF) is a think tank for future technologies and implementations for long-term groups to work on various aspects of the Internet. The ISOC provides leadership and training of the published Internet standards from the IAB and IETF. The [Internet Assigned Numbers Authority](#) (IANA) is responsible for global coordination of domain name resources and IP number addressing. The [Internet Corporation for Assigned Names and Numbers](#) (ICANN) is responsible for the domain name coordination and for registration and authorization of domain names. These are the main players in Internet governance, and as a business, you would need to engage these groups for additional or enhancements to current policies and technologies of the Internet.

## **Concerns**

These groups were created from United States government agencies, but there has been much international pressure in the past decade to move them to be more internationally focused.

## **Intranets**

### **Definition**

An intranet is an internal computer network accessible by an organization's employees. It uses Internet technologies and protocols so employees can access internal information through a browser without actually exposing that information to the broader Internet.

### **Business applications**

Generally, intranets support communication, collaboration and information search. An intranet can save on printing costs by serving as a document repository. Intranets can also be used as an alternative to e-mail, which can help save money on storage and bandwidth.

Intranet portals also can serve as an integration point for corporate systems. For instance, you can use the intranet as a way to access legacy systems or Web-enable internal applications. You can also [integrate enterprise user log-ons and authentication systems](#) with the intranet, giving employees one point of sign-on.

### **Deployment Concerns**

While intranets mimic the Internet in look and feel, their actual functionality and use have fallen short of expectations.

The biggest problem: getting employees to actually use them. A [2007 survey](#) by the Irish Computer Society found that 50 percent of respondents confessed they did not use company intranets.

Intranet consultant Martin White suspects one reason for the poor success of intranets is companies usually blindly deployed intranets, without first establishing concrete operational and strategic objectives. [White also noticed intranets are often treated as someone's hobby](#), and therefore lack serious oversight and management.

Intranets also fall short in search. Business users are accustomed to the ease and efficiency of online search tools such as Google. But online sites include coding and other [features that help search engines find and catalog information](#), a practice often neglected on intranet pages.

[Some](#) believe social networking, RSS and other Web 2.0 tools will revitalize struggling intranets, but it remains to be seen how that will play out long term.

## Intrusion-Detection Systems

### Definition

An intrusion-detection system gathers and analyzes information from a computer network or computer systems to identify unauthorized traffic that might be a malicious attack or misuse by an authorized user. If the information is deemed to be an attack or misuse, the intrusion detection system (IDS) sends an alert to pre-determined personnel to notify them of the incident.

### Business applications

Experts recommend that organizations [hosting publicly-accessible servers](#) deploy intrusion-detection systems behind a network firewall. By analyzing the traffic that makes it through the firewall, the IDS provide an extra measure of assurance that the traffic accessing the Web servers is not malicious. Organizations may also consider deploying an IDS on network segments that host critical systems to prevent unauthorized traffic from one network segment from accessing the critical systems on another segment.

### Deployment concerns

Intrusion-detection systems are susceptible to [false positives and false negatives](#) – traffic that is not malicious but is treated that way, and traffic that is malicious but is not recognized as such. IT personnel should regularly analyze IDS logs to correct false positives and false negatives, and make adjustments to the IDS to prevent the same instances in the future.

And that leads us to another challenge in deploying IDS. To get the most out of an intrusion-detection system, the organization must have a [knowledgeable analyst](#) monitoring its output and tuning it to the network environment. Analyzing log after log is often considered a mundane task, but to be done correctly, it requires extensive knowledge.



Intrusion-detection systems are frequently criticized for being passive and reactive. They identify unauthorized traffic but their capability to stop such traffic is limited. Thus, such systems increasingly are being packaged with intrusion-prevention systems, which are designed to actually prevent unauthorized traffic from accessing network resources.

Finally, like all security technologies, an IDS can be bypassed or attacked by savvy intruders. An IDS should be one element of a defense-in-depth strategy. While a properly tuned IDS can help identify the majority of attacks, it is not an end in itself.

### **Technical details**

An intrusion-detection system has three components: an analysis engine, sensors and a console. The sensors gather traffic information and send it to the analysis engine, which compares the traffic information against attack signatures and pre-defined rule sets. The final analysis is then sent to the console, which is often a GUI used by the IDS analyst to analyze the final data. Alerts can also be sent as a page or notifications on client systems used by the analyst.

There are several types of intrusion-detection systems, including network intrusion-detection systems and host-based intrusion detection systems. While a network IDS analyzes network traffic and monitors hosts, a host-based IDS examines application logs, system calls, file-system modifications and other host activities.

## **Intrusion-Prevention Systems**

### **Definition**

An intrusion-prevention system monitors network traffic and system activities to identify unauthorized or malicious use and prevent further action. For example, upon detecting a network attack, an intrusion prevention system (IPS) can drop the offending packets and prevent further communication from the source, while allowing all other traffic to traverse the network.

### **Business applications**

Some organizations are deploying intrusion-prevention systems in place of or in addition to intrusion-detection systems, which passively identify unauthorized traffic and are limited in their ability to react to such traffic. Thus, an [IPS may be deployed behind a firewall](#) to ensure that traffic from a public network, such as the Internet, does not threaten resources on the private network. An IPS also can be deployed on network segments that host critical systems to prevent unauthorized traffic from one network segment from accessing critical systems on another segment.

### **Deployment concerns**

Intrusion-prevention systems sit inline and are prevent attacks in real time. However, intrusion-prevention systems are more likely than intrusion-detection systems to [block legitimate traffic](#), and generate [false positives and false negatives](#) (traffic that is not malicious, but is treated that way, and traffic that is malicious but is not recognized as such). Some organizations consider this less of a risk than the possibility of damage caused by malware or an intrusion, and so accept the additional workload of analyzing false positives and false negatives.

Additionally, few IPSes can monitor encrypted traffic.

Like all security technologies, an IPS is susceptible to attack or can be bypassed by savvy intruders. For this reason, an IPS should be one of several security measures that organizations implement as part of a defense-in-depth strategy.

### **Technical details**

Like an IDS, an intrusion-prevention system has three components: an analysis engine, sensors and a console. The sensors gather traffic information and send it to the analysis engine, which compares the traffic information against attack signatures and pre-defined rules. The final analysis is then sent to the console, which is often a GUI used by the IPS analyst to analyze the final data. Alerts can also be sent as a page or notifications on client systems used by the analyst.

There are several types of intrusion-prevention systems, including network intrusion-prevention systems and host-based intrusion-prevention systems. While a network IPS analyzes network traffic and monitors hosts, a host-based IPS examines application logs, system calls, file-system modifications and other host activities.

Intrusion-detection and intrusion-prevention systems are increasingly being packaged together.

## **iPhone**

### **Definition**

In 2007, Apple Inc. began marketing its first smartphone, the [iPhone](#). The iPhone is a multimedia-enabled cell phone that also provides Internet connectivity, offers text messaging, serves as a portable media player, and camera phone. Users interface with the phone and its applications via a multi-touch screen that also offers a virtual keyboard for entering text.

As of today, there have been three versions of the iPhone released for use: the Original first generation, the 3G second generation, and the 3GS third generation. The iPhone has so far only been offered via the cellular phone carrier AT&T, with whom Apple has signed an exclusivity agreement.

The iPhone runs on its own operating system called iPhone OS, a modified version of the Darwin core of the Mac OS X. The phone is also managed via Apple's iTunes, which is how

Apple provides updates to the phone and allows users to purchase and download applications for the smartphone.

## **Business Applications**

Although many believe the iPhone isn't ready for the enterprise, small business owners and some enterprises have [welcomed the iPhone](#) and its wide variety of applications with open arms. [Recent reports show](#) that in 2009, Apple shipped nearly 2 million of its iPhone devices to corporate accounts. It seems that the iPhone is finding its niche in the [business smartphone market](#).

Features of the iPhone that business users find most useful include its multimedia applications. Some business-related applications are free to download, while others require a small fee. Even some large, well-known companies have created applications for the iPhone.

Some of the [top-rated business applications](#) in the Apple AppStore include Salesforce mobile, which allows users to access their customer database from their iPhones; Oracle Business Indicators software, which gives iPhone users access to human resources, financial and supply chain data; and Stage Hand, which allows iPhone users to control presentations from their smartphones.

## **Concerns**

There have been [several areas of concern](#) involving the iPhone, especially when it is used in the enterprise. Before buying the smartphone to use for work, one should consider its security issues, e-mail accessibility, calendar and contact sync capabilities, coverage area with the AT&T carrier, and battery life, among other possible issues.

The latest version of the iPhone has provided hardware-based encryption and a remote wipe capability—both of these improvements are welcome security provisions for the smartphone. However, experts warn that there are [still security issues](#) that are cause for concern. Before embracing the phone for enterprise use, it is recommended that the phone and its applications be [tested to ensure of the impact](#) of both on corporate data.

IT departments who will support the iPhone should also be sure that it is capable of synching with calendars and contact databases and that it works well with the e-mail software used in the organization. Also, users who travel may want to be sure that AT&T's network is available where they travel.

One other concern that business users must consider is the limitations on battery life for the iPhone. With normal use, the phone battery lasts around 5 hours before it must be recharged. Also, the battery is sealed inside the case of the iPhone, so users cannot swap out a dead battery with a charged one.

## **Technical Info**

The latest version of the iPhone, the [iPhone 3GS](#), is available in 16GB or 32GB form. Both versions include a 3-megapixel camera; 3.5” multi-touch screen; and uses UMTS/HSDPA, GSM/EDGE, Wi-Fi, and Bluetooth 2.1 connectivity.

The iPhone contains a sealed rechargeable lithium-ion battery with a 5-hour average talk-time on 3G networks. The phone provides up to 300 hours of standby time. To download system updates and applications, users are required to use iTunes 8.2 or later.

## **IPTV**

IPTV is the dissemination of programming using the Internet protocol. It usually, but not always, refers to delivery of the programming over the Internet.

IPTV is a broad category that is related to emerging IP-based video conferencing platforms. It can be used internally by an organization for training and meetings. It also can be a vehicle for reaching out to other businesses, customers and prospects. IPTV and IP video increasing competes with traditional cable and broadcast means to distribute entertainment and education programming. This competition goes two ways, as providers vie both for viewers and for deals with programmers.

## **Distribution**

There are a number of ways in which IPTV is disseminated, and each has its own concerns. The increase in available bandwidth is driving “over the top” IPTV. This is the provisioning of programming over unadorned broadband lines from websites such as [www.hulu.com](#). Such platforms run the risk of bandwidth shortages or other jitter- and latency-problems. More often than not, however, today’s networks adequately support the needs of general interest users. More specialized subscription services from service providers offer packages that have more robust delivery mechanism but are more expensive.

Of course, content also is finding its way to laptops, cell phones, smart phones and other mobile devices. Such services rely on 3G, Wi-Fi networks. The emergence of 3G and emerging WiMax and Long Term Evolution (LTE) platforms will increase the viability of mobile IPTV. Delivery over these networks, of course, introduces the relative strengths and weaknesses of each platform.

The distribution of movies, television shows and other content over the Internet radically alters the model that has existed, in more or less consistent form, since the introduction of commercial television after World War II. Of course, people will continue to get programming in the traditional manner. However, traditional broadcasting will be one of many options, not the sole option. The dislocation will be even greater than the changes brought by the emergence of cable television in the 1960s and 1970s.

The industry is beginning to serious deal with the issue of delivering IPTV to traditional televisions and not just computers. One element of the rollout involves functionality necessary in

the home to convert signals to formats usable by televisions. This circuitry can be located in standalone boxes, co-located in boxes with other functions or even sunken into sets themselves.

## ITIL

### Definition

The [Information Technology Infrastructure Library](#) (ITIL) is a set of policies and ideas for managing information technology infrastructure, development, and operations.

ITIL is a series of books; each covers a specific IT management topic. The United Kingdom's [Office of Government Commerce](#) (OGC) is the maintainer and trademark owner of the library. ITIL provides guidelines and policies for IT practices; however, it does not give exact details—that information is crafted for each organization adopting ITIL for use.

### Business applications

The goal of the policies and procedures within ITIL allow for reduced cost in an outsourced environment. It is suited to large enterprises that have disparate departments, but are seeking standardization and normalization of their IT departments. By [implementing the ITIL](#) methodologies and following its ideals, costs should be reduced overall within the organization and duplicate work should be eliminated.

### Controversies

ITIL advocates often believe that the ITIL library is an all-encompassing solution to IT problems. However, the library is merely a framework, and does not include all the answers for every organization. Because the library has a large focus on managing services provided to a customer, it has limited details and guidance on enterprise architecture and how those standards and designs reduce the impact on service organizations. The savings from the implementations of ITIL have yet to be seen.

### Technical details

The original goal of ITIL was to control costs, while outsourcing work for the UK government to third-party vendors. The Central Computer and Telecommunications Agency (CCTA) of the government controlled all purchasing of computers during the mainframe era. As PCs became more available, the various arms of the government began their own IT shops and needed guidance. They sought advice from the CCTA, who received advice from its vendors, and thus the library was started.

The original library was a set of books from IBM and because the binders that they were distributed in were yellow, they came to be known as the “[yellow books](#).” This is what matured into ITIL version one. The current version of ITIL is version three, and it contains information about strategy and continuing to improve upon existing processes.

## ITSM

### Definition

[IT service management](#) (ITSM) is a theory for IT system management that focuses on the area of customer relationships in respect to the way IT contributes to the business. Though it shares commonalities with other process improvement methodologies, it is not considered part of such frameworks. The ITSM process helps IT divisions to better interact with end-users and business customers in the sense that the IT staff provides these groups with a service.

### Business applications

ITSM as a practice enables the IT unit to consider the ways in which it provides services to other business units and its end users. Like other improvement methodologies, [its practice has grown quite popular](#) with enterprises in the past few years. However, ITSM does not typically include such IT-related groups as project managers or program managers, and in some cases software engineers. ITSM helps [IT align its services](#) more closely with the overall needs of the business, and it often helps IT staff to consider users as customers and systems as less operation-specific and more service-oriented.

### Concerns

Although the Information Technology Infrastructure Library (ITIL) includes ITSM as a component, ITSM is not synonymous with ITIL, though many still insist on using the two terms interchangeably. It is important to realize that ITSM and ITIL are two distinct disciplines.

### Technical details

Many process methodologies have contributed to the ITSM discipline, and several include examples of ITSM within their frameworks, including:

The Information Technology Infrastructure Library (ITIL)

IBM Tivoli Unified Process (ITUP)

Application Services Library (ASL)

Microsoft Operations Framework (MOF)

Business Information Services Library (BISL)

## LAN Network Protocols

This article discusses the campus protocols found in almost all enterprise networks today including spanning tree protocol, Ethernet and gigabit optical fiber with a description of the current specifications and process.

## **Spanning Tree Protocol**

Spanning Tree is an algorithm that runs on Layer 2 campus switches for preventing Layer 2 loops and broadcast storms on a network with at least 2 switches or bridges. The algorithm determines what ports at each switch or bridge must be blocked to create a loop free topology. Primary specifications are IEEE and 802.1d. The spanning tree port states are listening, learning, blocking, forwarding or disabled. Each group of switches will elect a root bridge as part of determining what switch ports must be blocked for a loop free topology. The root bridge is selected by default as the switch with the lowest priority (MAC address). Root bridge selection can be changed with the bridge priority command. It is important to consider your campus switch design and if necessary modify the root bridge selection for performance.

Newer switches that use VLAN's run one spanning tree instance per VLAN. This is important to note since Layer 2 loops occur per VLAN or segment. This allows a switch with dual connections to the same switch or different switches to load balance across those links without the concern of creating a broadcast storm. This is accomplished by assigning two VLAN's to a switch that has dual links to different campus core switches. Each link is configured to forward traffic from one VLAN and block it on the second link. For instance, consider a switch that is assigned 24 ports to VLAN 10 and 24 ports to VLAN 20 and a supervisor engine with 2 Gigabit ports that connect to different core switches. VLAN 10 is assigned to port A and VLAN 20 to port B. If traffic from VLAN 10 were allowed on port B as well, you would have a loop since traffic could leave on port A and return on port B assuming there is a trunk connection between the campus core switches.

## **Ethernet**

This is the most popular campus data link protocol running today. The primary specifications today are 10BaseT, 100BaseT, and Gigabit Ethernet. Many networks today are comprised of 10BaseT and 100BaseT from the desktop and server to the campus switch. Gigabit Ethernet is used from switch to switch and building-to-building. 10BaseT is a specification for 10 Mbps over unshielded twisted pair category 3 cable (UTP). The distance from desktop to switch is 100 meters maximum. The 100BaseT specification is the same except the speed is 100 Mbps over unshielded twisted UTP) pair category 5 cable. Gigabit is a specification for 1000 Mbps across Fiber, STP and UTP cabling. Ethernet uses CSMA/CD as a method of dealing with collisions when two desktops are sending data simultaneously. Both workstations wait for a specified and different length of time before attempting re-transmission. The maximum packet size or MTU of an Ethernet packet is 1518 Bytes.

## **Optical Fiber Technologies**

Gigabit Ethernet uses Multi-Mode Fiber (MMF) and Single Mode Fiber (SMF) for data transmission. Single Mode Fiber uses only one mode of light to travel across the fiber strand using a laser as the light source. Multimode allows for many modes of light to travel across the fiber strand at different angles using an LED as a light source. Modal dispersion results from different light modes transmitted across a fiber strand. The result is that Single Mode Fiber is higher bandwidth and transmits across greater distances. Multi-Mode Fiber is supported with

62.5 micron and 50 micron diameter fibers. The 50-micron fiber will transport across longer distances than 62.5 micron fiber. Multi Mode Fiber uses Short Wave Lasers (SX) and Long Wave Lasers (LX) for Gigabit transmission. Single Mode Fiber is supported with a 9 micron diameter fiber core. It uses long wave lasers to send data between buildings that are 10 kilometers apart.

## Linux Kernel

### Definition

The Linux kernel is the primary component of a Linux operating system whose basic function is to manage system resources. The kernel was the creation of [Linus Torvalds](#), a Finnish software engineer, who offered his kernel to the MINIX community board for help with completion of his “free” OS. The kernel has been used in many versions of the Linux operating system, called [distributions](#), which have been built by various contributors in the open-source community.

### Business applications

Because of its origins in the open-source community, many companies have been reluctant to accept the “free” Linux OS as a major component of their computer systems. But [more and more businesses](#) are giving the OS a chance to run on both their servers and their desktops.

There are also many Linux-based business [software applications](#). You can find applications such [accounting software](#), [project management software](#), and the [OpenOffice](#) software suite, all of which can be downloaded for free.

### Controversies

Linux has long been the source of controversy, such as the fear of using an open source OS in the enterprise, the possibility of [patent infringement](#), issues with [integrating Linux with Windows](#), and the actual [security of Linux servers](#). The OS has had an uphill battle, but it seems that it’s had some major victories—especially in the use of [Linux as a server operating system](#).

### Technical details

Linux versions are identified by a [four-number system](#) (i.e. 2.6.13.4). The first number indicated the kernel version; the second, the major revision of that kernel; the third is any minor revision to the kernel; and the last number indicates any emergency bug fixes or security patches.

Linus Torvalds, himself, sees to all major revisions to the latest kernel versions. There are usually [two versions of the kernel available for use](#): the stable version—indicated by even numbers in the second numeral, and the developmental version—indicated by odd numbers in the second numeral of the name. The developmental version usually changes because it is the version where developers are still working out the kinks on various new ideas being tested. The stable version remains the same, though.



## Litigation

### Definition

[Litigation](#), or a lawsuit, is the process by which a case goes before the court. When people or businesses have a dispute that cannot be resolved, the parties often enter into litigation and have their differences settled by a judge and/or jury.

The [steps involved in litigation](#) include the summons and complaint, the answer, case duration, preparation, discovery, motions, trial, decision, and appeal if necessary.

### Business applications

Both businesses and single parties can be involved in litigation. Also, there are various forms of litigation, some of which affect businesses more than others, including corporate litigation, personal injury, intellectual property, environmental, and labor and employment law.

### Concerns

In today's business world, there are [so many concerns](#) when someone brings up litigation. Depending upon the type of litigation, there could be issues with compliance of government regulations (i.e. Sarbanes Oxley) or e-discovery. In any case, it is important to be sure your legal counsel has a good relationship with your IT department to ensure a smooth transition of documents since most data in companies today are in digital formats.

## Mac OS

### Definition

Mac OS is an operating system developed for the Macintosh computer systems by Apple, Inc. The OS is graphical user interface-based—it lacks a command line; however, recent versions of the OS do allow a user to launch a terminal emulator to reach a command line.

### Business applications

Mac OS is probably best known for its use in the creative fields (e.g. digital imaging or graphic design), where Macs are pretty much the industry standard. But there are other reasons why this OS would make a great fit for your company.

One, its [Xcode](#) suite of development tools makes it an ideal development platform for [MySQL based applications](#) or other UNIX-based [development](#).

Two, [Security reliability](#), and [ease of setup and support](#) make it a great choice for businesses or schools.

And, finally, Mac OS provides [server applications](#) (e.g. web servers or application servers) that can run traditional UNIX applications.

## **Controversy**

Probably the biggest controversy in the Mac OS arena is that the Apple computers on which you run the OS are [more expensive](#) than a PC; however, that isn't always [the case](#). [Other arguments](#) in favor of the platform over Windows-based PCs are that the Macs are more secure, have less downtime, are easier to manage, and the computers can run Windows simultaneously with the Mac OS—all of which can add up to big savings in the long run.

In recent years, reports have also targeted Mac OS X for some [security issues](#). Those issues have been addressed in subsequent updates to the OS, but some have questioned [Apple's patch process](#) as being reactive rather than scheduled.

## **Technical details**

Mac OS is based on the original [NeXT OS](#) and a [BSD implementation of UNIX with a Mach kernel](#). Early versions of the Mac OS were referred to as the System software, but with the release of Mac OS 7.6 in 1997, Apple officially began calling it the [Mac OS](#). The most current version of the Mac OS is Mac OS 10.5, or [Leopard](#).

## **Managed Security Services**

### **Definition**

Managed security services are security operations outsourced to a company that specializes in those operations. Common managed security services include firewall management, vulnerability assessments, patch management, IDS management, e-mail security and content filtering, and intrusion response/forensics.

### **Business applications**

A managed security services provider does this work for organizations that choose not to maintain security operations or a portion of security operations in house due to cost, lack of expertise, desire to concentrate on core competencies, or the need for 24-hour service. Managed security services are a popular option for organizations that want to [co-source or out-task a portion of their IT efforts](#), so that the managed security service provider serves as an extension of the organization's IT staff.

### **Deployment concerns**

Choosing to engage in managed security services does not relieve the organization from responsibility. A [managed security service provider must be carefully chosen](#) with consideration given to the MSSP's experience in the organization's industry, accessibility (a

local presence should be preferred) and investment in current technology and trained personnel. The MSSP should be considered a partner in the organization's security efforts.

## Message Archiving

### Definition

Message archiving is a system wide method to protect and save electronic data in e-mail communications so it can be organized, searched, and accessed quickly at a later date.

### Business Applications

Historically, the user was responsible to keep copies of their e-mail messages, either by copying to disk, or printing them on paper to file. IT departments would back up the entire e-mail system, but only for catastrophic repairs--not to recall, or search single messages. A particular e-mail thread between two or more people could take days or even weeks to track down.

With the rise of regulatory and compliance laws, there became a need to find e-mail and trace its path within minutes. Policy based [archiving software](#) is available from many vendors, and allows messaging administrators to manage a large volume of e-mail data, as well as clean up space on production systems that increase performance. These software packages offer tools that allow indexing searching, and even the ability to trace e-mail threads between many users, which satisfy the newer legal discovery laws in the case that an e-mail chain is subpoenaed for use in court.

### Deployment Concerns

Archiving all of a company's e-mail can lead to a vast storage farm that can end up costing more than your messaging infrastructure. It is a good idea to seek the assistance of your legal and archiving software vendor for the best design and architecture for archiving. It may be necessary to only archive a small number of your users, or to expunge records after 1, 5 or 7 years. Some records may need to be archived indefinitely.

A software vendor may also have [best practices](#) on deployment to reduce the need for larger bandwidth in the servers, either in storage or networking. The need to duplicate all e-mail messages may also increase CPU load on your existing messaging servers, so a proper audit of existing servers would also be beneficial during the design process.

### Technical details

There are a large number of vendors and many e-mail systems that support message archiving. The basic process is that when a message comes in or out of the e-mail server, a duplicate is created. This duplicate message is then sent to a proprietary system that tags and indexes the message for later retrieval. This is transparent to the user.

Some software packages [allow the user](#) to retrieve archived messages, but not delete or alter them. If a purge time is set, a background process is used to comb through the archive and remove the old messages that are set to expire. Since this is done in line, it could--depending on the software--double the load on the server, network, and storage systems that are used in the messaging infrastructure.

## Net Neutrality

### Definition

[Net neutrality](#) refers to the general belief that on the Internet, there should be no restrictions placed on content that is viewed by users or on the applications, equipment, or platforms they use to view it. The basic idea behind the principle is that telecommunications companies must treat all Internet traffic equally.

Various advocates have developed a variety of definitions of the term. In 2005, the Federal Communications Commission developed its own [Broadband Policy Statement](#), which established four rules for continued open Internet usage and net neutrality. In this document, the FCC stated:

“To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to:

- Access the lawful Internet content of their choice.
- Run applications and use services of their choice, subject to the needs of law enforcement.
- Connect their choice of legal devices that do not harm the network.
- Competition among network providers, application and service providers, and content providers.”

### Controversies/Concerns

Telecom companies and Internet providers have long been battling against net neutrality. These companies claim they need to charge more for higher levels of services to be able to afford to keep up with technology advancements and upgrades that will permit Internet traffic to continue running.

Such service providers have recently proposed tiered levels of service, based on how much bandwidth a user consumes. The Internet service providers say that if net neutrality principles are followed, eventually they will have no choice but to raise rates or charge users per byte for their Internet usage.

Some experts have proposed that a [net neutrality tax](#) should be implemented to help carriers pay for the expensive upgrades and investments required to provide the level of Internet performance

to which users have grown accustomed. Taxpayers, though, have not been keen on the idea of paying more taxes, even if it does mean continued Internet improvements.

## **Business Applications**

So how does [net neutrality affect business](#)? If ISPs do manage to skirt net neutrality rules and raise their rates, most companies would be charged more for their Internet usage. Also, Internet-based companies might see less traffic if users are charged more just to visit their sites or use their online services.

For businesses, net neutrality has created a divided front. [Carriers and service providers](#) are now fighting against many [online companies](#) who fear losing money and users. Even the [European Union](#) and our own [U.S. congressmen](#) have joined the battle.

## **Technical Difficulties**

Because the Internet is considered to be a global entity, it is very difficult to impose regulations and rules upon it. The ongoing debate among Internet providers and carriers and the supporters of net neutrality is considered to be a U.S.-centric issue. Even within the U.S., though, there are thousands of Internet carriers, millions of companies who rely on the Internet for services and information, and over a billion users, which [complicate the debate on many levels](#).

So even if ISPs wanted to restrict or prioritize certain Internet packets, most Internet traffic crosses many carrier networks. So traffic from a user of a “premium” service may have packets traversing a “non-premium” network from another carrier. Not to mention data would travel among cable, DSL, and wireless services.

Also, who decides which packets take higher priority? Does e-mail deserve a lower level than voice traffic? And would critical services or applications be given priority over spam messages?

Since the early 2000s, many proposals have been made in the U.S. Congress to regulate net neutrality issues. Most have been killed, but some are still in discussion. The debate rages on.

## **Network Access Control**

### **Definition**

Network access control is a security technology designed to authenticate and prescreen clients before they access network resources to ensure that they comply with endpoint security policies. Based on the status of the endpoint, network access control (NAC) technologies may allow clients access to limited network resources, update them with proper security software (for example, antivirus or service packs), or deny them network access.

### **Business applications**

The traditional network perimeter has dissolved as organizations have opened their networks to business partners, offsite employees, contractors and guests. These parties can pose a risk if their endpoint devices do not have up-to-date antivirus software, patches, or personal firewall settings, or they access sensitive resources. Network access control allows organizations to extend network access to visitors while ensuring that the endpoint devices aren't introducing vulnerabilities into the network and while limiting access to specific resources.

## Deployment Concerns

Network access control sounds like a panacea, but the [technology is far from mature](#) and [not every company needs it](#). Experts recommend considering NAC if your organization is concerned about authenticating users or the security of the systems accessing the network, or if you need more granular access controls. If you do choose to implement the technology, then a phased deployment is recommended, beginning with IT.

Many experts are [skeptical of NAC's benefits](#), as the technology has yet to prove itself. [Several vendors have developed proprietary technology](#), but none has taken off or set a standard as the way network access control should be done. Its practicality has also been questioned in environments where a large number of diverse endpoints require network access.

## Technical details

Network access control systems can be installed inline or out-of-band. Inline NAC systems are often single-box appliances installed between users and the rest of the network and often require recabling. Out-of-band NAC systems reuse existing infrastructure, but also require changes to switches and routers. While inline systems can pose as a single point of failure, out-of-band systems offer the ability to manage one or multiple networks.

## Network Routing Protocols

### Overview

The purpose of routing protocols is to learn of available routes that exist on the enterprise network, build routing tables and make routing decisions. Some of the most common routing protocols include RIP, IGRP, EIGRP, OSPF, IS-IS and BGP. There are two primary routing protocol types, although many different routing protocols defined with those two types. Link state and distance vector protocols comprise the primary types. Distance vector protocols advertise their routing table to all directly connected neighbors at regular frequent intervals using a lot of bandwidth and are slow to converge. When a route becomes unavailable, all router tables must be updated with that new information. The problem is, with each router having to advertise that new information to its neighbors, it takes a long time for all routers to have a current accurate view of the network. Distance vector protocols use fixed-length subnet masks, which aren't scalable. Link state protocols advertise routing updates only when they occur, which uses bandwidth more effectively. Routers don't advertise the routing table, which makes convergence faster. The routing protocol will flood the network with link state advertisements to all neighbor routers per area in an attempt to converge the network with new route information. The

incremental change is all that is advertised to all routers as a multicast LSA update. They use variable length subnet masks, which are scalable and use addressing more efficiently.

## **Interior Gateway Routing Protocol (IGRP)**

Interior Gateway Routing Protocol is a distance vector routing protocol developed by Cisco systems for routing multiple protocols across small and medium-sized Cisco networks. It is proprietary, which requires that you use Cisco routers. This contrasts with IP RIP and IPX RIP, which are designed for multi-vendor networks. IGRP will route IP, IPX, Decnet and AppleTalk, which makes it very versatile for clients running many different protocols. It is somewhat more scalable than RIP since it supports a hop count of 100, only advertises every 90 seconds, and uses a composite of five different metrics to select a best path destination. Note that since IGRP advertises less frequently, it uses less bandwidth than RIP but converges much slower since it is 90 seconds before IGRP routers are aware of network topology changes. IGRP does recognize assignment of different autonomous systems and automatically summarizes at network class boundaries. As well, there is the option to load balance traffic across equal or unequal metric cost paths.

### **Characteristics**

- Distance Vector
- Routes IP, IPX, Decnet, Appletalk
- Routing Table Advertisements Every 90 Seconds
- Metric: Bandwidth, Delay, Reliability, Load, MTU Size
- Hop Count: 100
- Fixed Length Subnet Masks
- Summarization on Network Class Address
- Load Balancing Across 6 Equal or Unequal Cost Paths ( IOS 11.0 )
- Metric Calculation = destination path minimum BW \* Delay (usec)
- Split Horizon
- Timers: Invalid Timer (270 sec), Flush Timer (630 sec), Holddown Timer (280 sec)

## **Enhanced Interior Gateway Routing Protocol (EIGRP)**

Enhanced Interior Gateway Routing Protocol is a hybrid routing protocol developed by Cisco systems for routing many protocols across an enterprise Cisco network. It has characteristics of both distance vector routing protocols and link state routing protocols. It is proprietary, which requires that you use Cisco routers. EIGRP will route the same protocols that IGRP routes (IP, IPX, Decnet and Appletalk) and use the same composite metrics as IGRP to select a best path destination. As well, there is the option to load balance traffic across equal or unequal metric cost paths. Summarization is automatic at a network class address, however, it can be configured to summarize at subnet boundaries as well. Redistribution between IGRP and EIGRP is automatic as well. There is support for a hop count of 255 and variable length subnet masks.

### **Convergence**

Convergence with EIGRP is faster since it uses an algorithm called dual update algorithm or DUAL, which is run when a router detects that a particular route is unavailable. The router queries its neighbors looking for a feasible successor. That is defined as a neighbor with a least-cost route to a particular destination that doesn't cause any routing loops. EIGRP will update its routing table with the new route and the associated metric. Route changes are advertised only to affected routers when changes occur. That utilizes bandwidth more efficiently than distance vector routing protocols.

## **Autonomous Systems**

EIGRP does recognize assignment of different autonomous systems, which are processes running under the same administrative routing domain. Assigning different autonomous system numbers isn't for defining a backbone such as with OSPF. With IGRP and EIGRP, it is used to change route redistribution, filtering and summarization points.

## **Characteristics**

- Advanced Distance Vector
- Routes IP, IPX, Decnet, Appletalk
- Routing Advertisements: Partial When Route Changes Occur
- Metrics: Bandwidth, Delay, Reliability, Load, MTU Size
- Hop Count: 255
- Variable Length Subnet Masks
- Summarization on Network Class Address or Subnet Boundary
- Load Balancing Across 6 Equal or Unequal Cost Paths (IOS 11.0)
- Timers: Active Time (180 sec)
- Metric Calculation = destination path minimum BW \* Delay (msec) \* 256
- Split Horizon
- LSA Multicast Address: 224.0.0.10

## **Open Shortest Path First (OSPF)**

Open Shortest Path First is a true link state protocol developed as an open standard for routing IP across large multi-vendor networks. A link state protocol will send link state advertisements to all connected neighbors of the same area to communicate route information. Each OSPF-enabled router, when started, will send hello packets to all directly connected OSPF routers. The hello packets contain information such as router timers, router ID and subnet mask. If the routers agree on the information, they become OSPF neighbors. Once routers become neighbors, they establish adjacencies by exchanging link state databases. Routers on point-to-point and point-to-multipoint links (as specified with the OSPF interface type setting) automatically establish adjacencies. Routers with OSPF interfaces configured as broadcast (Ethernet) and NBMA (Frame Relay) will use a designated router that establishes those adjacencies.

## **Areas**



OSPF uses a hierarchy with assigned areas that connect to a core backbone of routers. Each area is defined by one or more routers that have established adjacencies. OSPF has defined backbone area 0, stub areas, not-so-stubby areas and totally stubby areas. Area 0 is built with a group of routers connected at a designated office or by WAN links across several offices. It is preferable to have all area 0 routers connected with a full mesh using an Ethernet segment at a core office. This provides for high performance and prevents partitioning of the area should a router connection fail. Area 0 is a transit area for all traffic from attached areas. Any inter-area traffic must route through area 0 first. Stub areas use a default route to forward traffic destined for an external network such as EIGRP since the area border router doesn't send or receive any external routes. Inter-area and intra-area routing is as usual. Totally stubby areas are a Cisco specification that uses a default route for inter-area and external destinations. The ABR doesn't send or receive external or inter-area LSA's. The not-so-stubby area ABR will advertise external routes with type 7 LSA. External routes aren't received at that area type. Inter-area and intra-area routing is as usual. OSPF defines internal routers, backbone routers, area border routers (ABR) and autonomous system boundary routers (ASBR). Internal routers are specific to one area. Area border routers have interfaces that are assigned to more than one area such as area 0 and area 10. An autonomous system boundary router has interfaces assigned to OSPF and a different routing protocol such as EIGRP or BGP. A virtual link is utilized when an area doesn't have a direct connection to area 0. A virtual link is established between an area border router for an area that isn't connected to area 0, and an area border router for an area that is connected to area 0. Area design involves considering geographical location of offices and traffic flows across the enterprise. It is important to be able to summarize addresses for many offices per area and minimize broadcast traffic.

## **Convergence**

Fast convergence is accomplished with the SPF (Dijkstra) algorithm, which determines a shortest path from source to destination. The routing table is built from running SPF, which determines all routes from neighbor routers. Since each OSPF router has a copy of the topology database and routing table for its particular area, any route changes are detected faster than with distance vector protocols and alternate routes are determined.

## **Designated Router**

Broadcast networks, such as Ethernet, and Non-Broadcast Multi Access networks, such as Frame Relay, have a designated router (DR) and a backup designated router (BDR) that are elected. Designated routers establish adjacencies with all routers on that network segment. This is to reduce broadcasts from all routers sending regular hello packets to its neighbors. The DR sends multicast packets to all routers that it has established adjacencies with. If the DR fails, it is the BDR that sends multicasts to specific routers. Each router is assigned a router ID, which is the highest assigned IP address on a working interface. OSPF uses the router ID (RID) for all routing processes.

## **Characteristics**

- Link State
- Routes IP
- Routing Advertisements: Partial When Route Changes Occur
- Metric: Composite Cost of each router to Destination (100,000,000/interface speed)
- Hop Count: None (Limited by Network)
- Variable Length Subnet Masks
- Summarization on Network Class Address or Subnet Boundary
- Load Balancing Across 4 Equal Cost Paths
- Router Types: Internal, Backbone, ABR, ASBR
- Area Types: Backbone, Stubby, Not-So-Stubby, Totally Stubby
- LSA Types: Intra-area (1,2) Inter-area (3,4), External (5,7)
- Timers: Hello Interval and Dead Interval (different for network types)
- LSA Multicast Address: 224.0.0.5 and 224.0.0.6 (DR/BDR) Don't Filter !
- Interface Types: Point to Point, Broadcast, Non-Broadcast, Point to Multipoint, Loopback

## **Integrated IS-IS**

Integrated Intermediate System - Intermediate System routing protocol is a link state protocol similar to OSPF that is used with large enterprise and ISP customers. An intermediate system is a router, and IS-IS is the routing protocol that routes packets between intermediate systems. IS-IS utilizes a link state database and runs the SPF Dijkstra algorithm to select shortest paths routes. Neighbor routers on point to point and point to multipoint links establish adjacencies by sending hello packets and exchanging link state databases. IS-IS routers on broadcast and NBMA networks select a designated router that establishes adjacencies with all neighbor routers on that network. The designated router and each neighbor router will establish an adjacency with all neighbor routers by multicasting link state advertisements to the network itself. That is different from OSPF, which establishes adjacencies between the DR and each neighbor router only. IS-IS uses a hierarchical area structure with level 1 and level 2 router types. Level 1 routers are similar to OSPF intra-area routers, which have no direct connections outside of its area. Level 2 routers comprise the backbone area, which connects different areas similar to OSPF area 0. With IS-IS, a router can be an L1/L2 router, which is like an OSPF area border router (ABR), which has connections with its area and the backbone area. The difference with IS-IS is that the links between routers comprise the area borders and not the router. Each IS-IS router must have an assigned address that is unique for that routing domain. An address format is used, which is comprised of an area ID and a system ID. The area ID is the assigned area number and the system ID is a MAC address from one of the router interfaces. There is support for variable length subnet masks, which is standard with all link state protocols. Note that IS-IS assigns the routing process to an interface instead of a network.

## **Characteristics**

- Link State
- Routes IP, CLNS
- Routing Advertisements: Partial When Routing Changes Occur

- Metric: Variable Cost (default cost 10 assigned to each interface)
- Hop Count: None (limited by network)
- Variable Length Subnet Masks
- Summarization on Network Class Address or Subnet Boundary
- Load Balancing Across 6 Equal Cost Paths
- Timers: Hello Interval, Hello Multiplier
- Area Types: Hierarchical Topology similar to OSPF
- Router Types: Level 1 and Level 2
- LSP Types: Internal L1 and L2, External L2
- Designated Router Election , No BDR

## **Border Gateway Protocol (BGP)**

Border Gateway Protocol is an exterior gateway protocol, which is different from the interior gateway protocols discussed so far. The distinction is important since the term autonomous system is used somewhat differently with protocols such as EIGRP than it is with BGP. Exterior gateway protocols such as BGP route between autonomous systems, which are assigned a particular AS number. AS numbers can be assigned to an office with one or several BGP routers. The BGP routing table is comprised of destination IP addresses, an associated AS-Path to reach that destination and a next hop router address. The AS-Path is a collection of AS numbers that represent each office involved with routing packets. Contrast that with EIGRP, which uses autonomous systems as well. The difference is their autonomous systems refer to a logical grouping of routers within the same administrative system. An EIGRP network can configure many autonomous systems. They are all managed by the company for defining route summarization, redistribution and filtering. BGP is utilized a lot by Internet Service Providers (ISP) and large enterprise companies that have dual-homed Internet connections with single or dual routers homed to the same or different Internet Service Providers. BGP will route packets across an ISP network, which is a separate routing domain that is managed by them. The ISP has its own assigned AS number, which is assigned by InterNIC. New customers can either request an AS assignment for their office from the ISP or InterNIC. A unique AS number assignment is required for customers when they connect using BGP. There are 10 defined attributes that have a particular order or sequence, which BGP utilizes as metrics to determine the best path to a destination. Companies with only one circuit connection to an ISP will implement a default route at their router, which forwards any packets that are destined for an external network. BGP routers will redistribute routing information (peering) with all IGP routers on the network (EIGRP, RIP, OSPF, etc.), which involve exchange of full routing tables. Once that is finished, incremental updates are sent with topology changes. Each BGP router can be configured to filter routing broadcasts with route maps instead of sending/receiving the entire internet routing table.

## **BGP Routing Table Components**

- Destination IP Address / Subnet Mask
- AS-Path
- Next Hop IP Address

## Network Security

### Definition

Network security is a collective term that refers to the hardware, software and procedural methods used to protect a computer network infrastructure and the systems on it. Computer networks can be vulnerable to many threats, including unauthorized access, which can lead to confidentiality breaches, disruption of business operations due to loss of network availability, and data tampering or destruction.

### Business applications

Network security is a complex effort that involves many technologies to provide defense-in-depth. Experts suggest approaching network security by [first identifying everything that is on the network](#). Once you know what needs to be protected, you can determine how to protect it based on your company's risk profile.

Best practices dictate that network security should include some standard technologies and procedures:

- Antivirus to prevent malicious code from infecting network systems.
- Firewalls to inspect incoming and outgoing network traffic.
- Strong passwords changed periodically to authenticate users.
- Routers and switches configured appropriately.
- Operating systems kept up to date with patches.
- Security-awareness training for users, including physical security.
- A network analyzer or monitoring device to inspect traffic.

Other countermeasures include content filtering, encryption, virtual private networks, anti-spyware, intrusion-detection and –prevention systems, network access control and unified threat management.

### Deployment concerns

The [biggest threat to network security](#) also happens to be one that is often overlooked – the user. Businesses need to be mindful of the possibility of internal breaches. In unauthorized access, it doesn't matter whether the intruder is on the company payroll. Keep access control lists current and use appropriate authentication methods.

The value of a network inventory cannot be overstated. Businesses cannot protect what they don't know exists. Make network inventories a regular practice.

As in e-mail security, dropping a single piece of technology on the network is not going to provide complete protection. A traditional network firewall is a vital piece of network security, but it doesn't stop there. Businesses should take a layered approach to network security, building security countermeasures throughout the network for defense-in-depth.

## **Technical details**

Firewall manufacturers are increasingly integrating network security technologies in what are referred to as [unified threat management](#). Unified threat management offers the benefit of multiple technologies under one hood – or dashboard, as the case may be. This is meant to simplify the installation and management of various technologies while providing protection against a variety of threats. Unified threat management products usually include antivirus, network firewall, content filtering and anti-spam. Advanced features include intrusion detection/prevention, virtual private network and Web application scanning.

## **Network Topology**

### **Hierarchical Model**

A hierarchical model is a modular design for an enterprise network that defines three specific layers, which each have network services associated. The layers are access, distribution and core. The access layer is associated with branch offices that usually run lower-speed circuits. These branch offices are aggregated at a distribution office and several distribution offices are aggregated at a core office. Modular designs are more scalable and utilize bandwidth more effectively than flat networks.

### **Access Level Services**

Static Routing, Encryption, Compression, Load Balancing, Access Control Lists, VLAN's, Proxy Services, Queuing

### **Distribution Level Services**

Summarization, Redistribution, Network Address Translation, Protocol Translation, Quality of Service, Inter-VLAN Routing, Access Control Lists (applications, protocols and services)

### **Core Level Services**

Traffic Optimization, Path Optimization, Encapsulation, Quality of Service, Load Balancing

## **Topologies**

The following describes the most common network WAN topologies implemented in an enterprise environment.

### **Hub and Spoke**

Each spoke has one or more links to a hub office that will connect the spoke offices. It is the least expensive and easiest to manage. There isn't any circuit diversity unless backup circuits are provisioned at each office. If a circuit fails at a spoke office and there is no backup circuit, that spoke office is without network access.

## **Partial Mesh**

With a partial mesh topology, any office could be designated as a hub office. This is more expensive than hub and spoke since there are alternate circuits to different offices. If one link fails, that doesn't affect any office since a new route will be discovered with the routing protocol. The bandwidth at each circuit will affect what preferred routes are selected under normal operating conditions.

## **Full Mesh**

This is the most expensive topology type since there is any-any connectivity among all offices. It is the most difficult to manage, although most reliable with multiple paths to any destination. For companies such as banks that require 99.999% availability, this topology would be employed.

## **Open Data Standards**

### **Definition**

Open Data Standards are data standards that are open source rather than proprietary. Open data standards are written by groups or organizations, publicly documented and must be freely available for adoption.

There are literally tens of thousands of open data standards identified by the International Organization for Standardization. Most are written by industry-specific groups. Examples of industry-specific data standards group include the Public Health Data Standards Consortium, a Pipeline Open Database Standard Association and the National Geospatial Program.

Some standards, however, are open and adopted across industries. The Consortium for Open Source Software in Public Administration [published a useful glossary on data standards](#), which lists the following open source data standards:

1. Comma Separated Values
2. TeX
3. XML
4. HTML
5. RDF
6. DocBook
7. ebXML
8. Scalable Network Graphics
9. XSL-FO
10. Simple Text
11. Portable Network Graphics (binary)
12. JPEG (binary)

## **Business applications**

Data standards are specifications that ensure interoperability. By following data standards, organizations can easily share data from business partners and customers.

## OSI Network Model

### Enterprise Networking Defined

An enterprise network is a large network comprised of hundreds or thousands of workstations all connected with WAN circuits across many states and/or countries. The components are comprised of network devices, circuits, servers, applications, security and network management that connect employees for the purpose of supporting business processes. It is business processes that make companies profitable.

The leveraging of new technologies to reduce costs and increase revenue is a business strategy that many companies have employed recently. That is contrasted with the Internet Service Provider (ISP) market, which refers to companies whose business it is to sell infrastructure, Web hosting and application services to small, medium and enterprise companies. Many enterprise companies now rely on ISP for some or all of the mentioned components that comprise an enterprise network. Usually all circuits are provisioned with the ISP. Some devices are ISP owned and the servers and applications can be all ISP owned if you have a hosting agreement with them that provides those services. Management and security of your network can be outsourced to an ISP as well, which is becoming popular with many Fortune 500 companies. Examples of that are AT&T and IBM, who offer outsourcing agreements with many services and options.

### OSI Model as a Phone Call

The OSI model was developed years ago as a reference for network protocol and application designers to build their products with an open standard. That would promote a standard for developing network devices, interfaces, applications and services that would work together. It is a model rather than a specification since it defines layers and services for those layers and how each layer works with the layer above and below it.

The model is a representation of how a network operates, much the same as a phone call. A phone call from your home to a particular destination requires a physical connection that electrically connects those two locations. When you take your phone off the hook to make a call, that is similar to layer 1 physical and layer 2 data link services. When you dial a number, that is a layer 3 network service or phone number routing. When someone answers the phone call, that is similar to layer 4 transport and layer 5 session services with talking and listening. The specific language that you are speaking is layer 6 presentation and layer 7 application services. Today's data networks use similar design principles.

### OSI Layers and Your Business Network

Your desktop computer at work is connected to an application server over a physical media such as unshielded twisted pair (UTP) cable. That layer 1 service is the electrical signaling from your desktop to a campus switch and from a campus switch to a server. Your desktop network interface card connects your desktop to the network cable and uses a layer 2 data link protocol such as Ethernet that establishes a connection with the campus switch and defines when that desktop has access to the network.

Before sending data, the desktop must know the address of the server to which it is sending data. That is a layer 3 network service. The layer 4 transport service establishes a logical connection between server and desktop for coordinating traffic flow. As well, layer 4 does error correction and re-transmission of packets if there are problems with data delivery. With the data connection established, it is the layer 5 session service that maintains a logical connection between application processes at the desktop and server. The formatting of the data for a particular application is a layer 6 presentation service. Many applications will utilize their own formatting, which is something you learn when you open files from different word processing vendors. The application interfaces with the OSI model at layer 7, which is the application layer. This level defines an API that applications use to develop their specific applications that will work with that layer.

## **OSI Model and Microsoft Windows**

The development of open industry standards at various layers of the OSI model has contributed to the proliferation of multi-vendor network integration. Some examples of application layer services are FTP, Telnet, SNMP and many applications that are used over a typical network.

Microsoft has done a lot of work to standardize its Windows platform API so that third-party application developers can write programs for that operating system. When you examine Windows 2007, for instance, you will notice that it provides services at layers 3 - 7 of the OSI model. The argument could be made that Microsoft is involved with layer 1 and layer 2 services as well, since there are some software drivers for network interfaces that are available from it.

Describing client network software from Microsoft that runs at each desktop is describing all of the programs such as protocol stacks, network interface card drivers, and programs that integrate these elements. The network driver software is typically found at layer 1 through layer 4, while application developers will focus on layers 5 - 7 of the OSI model.

It should be noted that the OSI model is a model, which suggests that it provides guidelines for network developers. Some network software, such as SNA, does not define a network layer 3. The result is that it is not routable and a service such as encapsulation or tunneling must be used at the router for sending data across a network that is using a network layer and associated IP addressing. An example is integrating an SNA network, which doesn't have a network layer, with a Windows network using IP network services.



## OS Interoperability

### Definition

OS interoperability is ability for different operating systems to share user data using common protocols. This allows users to work in a homogenous environment, moving from platform to platform with little or no rework.

### Business applications

Interoperability between OSs is key in the enterprise where servers might run Linux, while desktops run on Windows or another OS, yet all are able to exchange information. Another way that interoperability is important in the workplace would be where some computers run [Linux or MacOS and others run Windows](#), yet all users can exchange documents and work together smoothly.

### Controversy

There have been many issues involving problems with interoperability—most recently between [Linux and Windows](#). Microsoft has had [many legal issues](#) with open-source, noncommercial software that uses its protocols to provide the necessary interoperability with Windows. They have pledged to work to lessen such [interoperability issues](#), but many have not been impressed with what has been done so far.

### Technical details

To [ensure that systems can work together](#), there are many factors to be considered, including system-level design and network protocols. Adhering to the standards can ensure that all computers communicate properly, but there are also other levels of interoperability to weigh (i.e. even if the OSs can communicate, are the software products being used able to interpret the data in the same ways?).

## OS Migration and Testing

### Definition

An [OS migration process](#) is when you change or upgrade the operating system on your computer. It can take from a few minutes to a few months of planning and usually requires testing of your current applications on the new OS to be sure everything will work smoothly once the migration is complete.

### Business applications

Most every business will go through a migration at some point. The [reasons to migrate](#) to a new or different OS could be to save money, to merge together two IT operations (as in a merger of companies), or to provide new technologies that aren't available with your current OS.

When planning a migration, it's important to test all current software being used on your old OS to ensure that they work with the new OS and also to find out if there will be any issues that might cause users to need detailed support when they first begin using the new OS.

## **Controversy**

There is a reluctance to change in a support organization to newer or different OSs because often a change in the OS usually requires a re-education of support personnel and retooling of IT support processes. The new operating system, however, may have fewer problems than the previous one, thereby reducing the amount of support calls and issues that users face, or it may provide more security fixes or increase productivity.

## **Technical details**

Often, IT departments prefer to wait to upgrade computers to a new OS. Many site the need for testing and preparation. But there are also quite a few who claim that waiting for the company to [“work out the bugs” before they upgrade](#) is worth it. The key is knowing whether the immediate upgrade is necessary or if it will provide benefits that outweigh any problems incurred during the change.

## **Patch Management**

### **Definition**

Solutions to the security of an enterprise justify the development of a patch-management plan. Patch management puts the security of your data and networks ahead of hackers' attempts to thwart that security. Enterprises consider patch management a vital tool.

### **Business Applications**

Keeping on top of vulnerabilities is vital to security and the infrastructures of businesses. But, the work of applying patches is slow and inconsistent. Without a management plan enterprises have seen a massive exploitation of vulnerabilities even after the patch has been released.

When it comes to patching security vulnerabilities, time is of the essence. The slow and inconsistent nature of applying patches has led to massive exploitation of vulnerabilities even after the patch has been released. Keeping on top of vulnerabilities is vital to security and infrastructure of businesses. (See [Patch Management Is a Full-Time Job.](#))

## Security Issues

[A Red Light Security blogger makes the point](#) that patch management becomes more complex and perhaps even more vital in a virtualized world. He advocates keeping the host OS patched and hardened, which activates virtual machine security. Then, scan regularly for vulnerabilities establishing policies, standards and procedures, and watching for useful third-party products.

## Technical Details

Many patches that are available take a while for IT to apply. Why is this? Because the IT employees have to search for the patches and there exists the fear that the patches themselves may cause their own further problems. But, security vulnerabilities will let you know when they're breached. So, there needs to be a plan in place for keeping abreast of available protections for infrastructures. Companies also must factor in the cost of operating-system support and utilities for managing agents.

## PCI Data Security Standard

### Definition

The PCI Data Security Standard is a set of policies and requirements for increasing credit card account data security. The standard was developed by the [PCI Security Standards Council](#), which includes American Express, Discover Financial Services, JCB International, MasterCard

Worldwide and Visa International. It was created to help companies that work with financial customer data adopt a consistent data security policy internationally.

### Business applications

These policies are for interacting with most credit card processing companies. Companies that work with [credit card data](#) should already have most, if not all of these policies in place already. However the PCI DSS formalizes the documentation of the policies that are used to meet the requirement of certification of data security.

### Concerns

As with any security documentation, it is not valid if it is not frequently updated and implemented in production systems as documented in the standards. The most important part of deployment of new security standards is the audit, which validates that the system administrators and programmers who must abide by the new rules are following them and updating internal documentation to reflect the new policies.

### Technical details

The core ideals of the PCI DSS are straightforward, and to most security experts make rational sense. This list is taken from the PCI website that defines the [technical requirements](#) of the policy:

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Requirement 3: Protect stored card holder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

## Privacy

### Definition

[Privacy](#) regards the amount of information that a person or organization wishes for the outside world to access. People's views of what is considered to be private vary, but there are laws to govern certain aspects of personal privacy.

The very term “privacy” can also take on different meanings within different contexts. For example, physical privacy might concern a person's physical space or body; organizational privacy would relate to companies, agencies, or organizations that wish to keep activities secret; and informational privacy might deal with keeping data about a person or an organization away from others who might try to misuse such information.

### Business applications

In terms of business and technology, most thoughts about privacy relate to [informational or data privacy](#). In the Internet age, privacy battles have ensued in the areas of music, movies, healthcare records, and even financial data. Many [government acts and laws](#) have been passed to protect such integral information. Companies must often meet rigorous compliance measures to ensure that its data, in all its forms, is kept safe.

## Concerns

Of course, in terms of privacy, the largest concern is how to protect it. The most globally accepted explanation of a human's rights of privacy is spelled out in the [Universal Declaration of Human Rights](#). In the United States, personal privacy is governed by the [Privacy Act of 1974](#).

## Product Recall

### Definition

A [product recall](#) occurs when a manufacturer or consumer finds a defect in a product that has or will cause injury to people consuming or using the product. This is not limited to a single industry, and it has happened in almost all industries, from automobiles to food. Product recalls usually end with the manufacturer giving back the consumer their money or a new fixed product, free of charge.

### Business applications

In the United States, the [U.S. Consumer Product Safety Commission](#) (CPSC) is the government agency that oversees consumer product recalls on behalf of the consumer. It also works with the manufactures to ensure that their products are safe for sale. The [National Highway and Transportation Safety Association](#) (NHTSA) oversees the recalls and safety equipment for automobiles. There are other organizations, such as the Food and Drug Administration, the U.S. Coast Guard, and the Environmental Protection Agency, that have parts in the recall of products to prevent injury and harm. The U.S. government also offers a website, [Recalls.gov](#) that provides a singular access to all of these organizations. Businesses are also under the watchful eye of many third party groups (i.e. the [Public Interest Research Groups](#)) that monitor and manage product testing to validate that items up for sale are safe for the people who will use them.

## Concerns

The biggest concern about product returns is that often, a measurable amount of injury occurs before recalls are normally done. In a rush to get products to market, some companies may abbreviate testing and safety standards to increase profit, which can ultimately lead to injuries and recalls.

## Project Management

### Definition

[Project management](#) involves managing the process of directing a team or group to complete a specific goal or project. Project management requires identifying the objectives, creating a plan, and managing all resources to meet or exceed the goals of the project within the constraints of time, budget, and scope.

The discipline of project management harkens back to the late 1800s to early 1900s when [Frederick Winslow Taylor](#) identified his theories of scientific management. Followers of those theories, [Henry Gantt](#) and [Henri Fayol](#), are also accredited with furthering project management with their own contributions. Gantt developed the Gantt chart; Fayol created his five management functions, which are the embodiment of the project and program management theories.

### **Business applications**

Any business could use [project management](#) practices to complete large projects and goals. Though most project management jobs are found in such fields as engineering, construction, information technology, and defense, where large-scale projects take months or years to complete and require detailed organization and scheduling to meet strict deadlines.

### **Technical details**

Within project management, there are [several methodologies](#) for managing projects, including: Adaptive Project Framework, Extreme Programming, TenStep, Rational Unified Process, Systems Development Life Cycle, and PRINCE2.

Within these methodologies, most projects will have [similar stages](#): initiation, planning and development, production, monitoring and control, and closing.

## **Remote Administration**

### **Definition**

Remote Administration covers many topics in data-center operation and desktop management. For example, [the way applications are deployed affects budgets](#). Nick Sanna of Netuitive suggests applications better be accessible and perform well for users at all times. So, performance monitoring is pretty important. However, the only monitoring tools that IT managers seem to rely on these days are complaining customers. Such a tool is an undependable alert system. As a result, most problems go undetected until it's too late.

### **Business Applications**

In fact, a recent survey by Gartner showed that 70 percent of IT managers have little or no confidence in their current systems-management tools. That's because the traditional monitoring tools rely on manual guesswork for setting monitoring thresholds and analyzing performance. It's not just that automation can make these tools better—but that without it, they can never work well at all. Netuitive has a solution that adds automated analysis to already installed monitoring

tools. This self-learning, performance-management software automates 90 percent of manual systems administration tasks and isolates root causes automatically.

While these solutions aren't cheap, there is substantial ROI, sometimes in just a few months. Netuitive has a customer that had 10 full-time people dedicated to performance monitoring and was able to reduce this number to just one administrator after the software was deployed.

### **Administering user permissions**

Privileged user accounts are the most powerful accounts defined within critical applications and the servers, operating systems and databases on which they run. These include, but are not limited to, generic accounts such as Administrator on Wintel platforms, Root on UNIX systems, Cisco Enable, DBA passwords, and the hard-coded passwords found in application scripts throughout an enterprise.

These accounts provide wide-ranging access to the data within the application/system, the ability to view/copy/modify this highly sensitive information, and even the ability to change the access rights to this information. If the accounts are not properly managed and secured, with the default passwords changed to a strong password, and under a trackable "change control" process/system, it leaves these critical applications and the data they contain vulnerable to deliberate or inadvertent misuse, breaches and potential data theft.

### **Deployment Concerns**

A company called [NetSupport](#) has released a new version of its NetSupport Manager that extends remote control, deployment and other services to 32-bit and 64-bit Vista environments.

### **Security Issues**

An important question to ask remote-service providers revolves around the issue of security. Brian Anderson, vice president of marketing for [Axeda](#), a provider of secure remote service and support capabilities, says that with security, he does an annual security audit by VeriSign. That's something people should ask about—not only if a company says it's secure, but if it can prove it.

### **Technical Details**

There are [several common mistakes](#) that are made when dealing with privileged user identities and passwords:

- 1) Not being aware of all of the default accounts on target machines, systems and applications.
- 2) Not changing the default passwords on all of the privileged user accounts on these targets.
- 3) Making these passwords easy to remember and/or generic across multiple systems.

4) Having the privileged identities/passwords written down or visible in publicly or easily accessible areas.

5) Trusting the IT team — i.e., allowing all system administrators to have access/know all administrative passwords.

6) Hard-coded passwords in test scripts, application scripts, et al.

In today's business environment, applications need to "log into and access" other applications constantly, such as, in Cyber-Ark's Enterprise Password Vault. Here's how control and auditing of the actions of authorized users is handled.

When the Enterprise Password Vault is implemented, there are several types of user created on the system. These include:

1) Vault Administrator Users, who have the ability to add users to the Vault, create Safes in the Vault (the logical unit of management within the Vault—Safes contain files and objects), run reports, set access rights and do other administrative functions within the Vault.

2) Audit Users, who do not have the same abilities as the Vault Administrator to add users, create Safes, etc, but have the ability to run reports and audit accesses to the vault, individual Safes (of which they are a named audit "owner") and of the files within these Safes.

3) General Users, of which there are two types: Safe Owners and Safe Users. A Safe Owner has the ability to allow existing Vault users to have access to the Safes they own, and manage the information, rights and monitoring of those Safes.

## Request for Proposals

### Definition

A Request for Proposal, or RFP, is an invitation for providers of a service or product to bid on the right to supply the service or product to the entity issuing the RFP.

### Business applications

RFPs provide structure to all stakeholders in the process, but particularly allow the issuing entity (a business, for instance) to:

- Get accurate information on which to base decisions.
- Have a broader range of solutions.
- Get the best deal by leveraging purchasing power.
- Make appropriate strategic procurement decisions.



For the company or entity submitting the RFP, a well-constructed RFP:

- Makes it clear what the company wants to purchase.
- Makes wide distribution and response possible.
- Demonstrates impartiality through its structure and evaluative quality, which can be extremely important in public-sector contexts.
- Lets suppliers know that your company is looking to obtain their offerings and encourages high-quality effort.
- Signals to suppliers the competitive nature of the process.
- Promotes factual responses from suppliers.

## **Concerns**

Increasing use of RFPs has led to an rise in the need for resources that help both issuing entities and suppliers understand, react to and implement them. According to IT Business Edge's Patrick Avery:

...business professionals [are] desperate for more information on how to succeed in a system that seems to cater more to large companies looking for free consulting than to vendors hoping to land new accounts.

## **Risk Management**

### **Definition**

[Risk management](#) involves investigating, alleviating, and policing potential risks. To perform risk management, it is important to consider risks from all angles including disasters, attacks, failures, etc.

### **Business Applications**

Although it seems impossible to prevent uncertain threats from occurring, a company must have its own strategy in place for managing business in the face of a threat or avoiding the risks altogether. It is important to [assess risks throughout your business](#).

In the IT sector, computer systems and networks are relied on heavily, so [identifying and managing risks](#) to those systems is important to the success of your business. For example, in a healthcare related business, it would be extremely important to mitigate the risk of data loss and privacy issues. A business that relies on its Website for sales, however, would want to minimize or eliminate any downtime for their Website.

All businesses must realize some level of risk, though, no matter what types of plans are in place to mitigate or alleviate them. Some risks cannot be avoided.

## **Concerns**

In many business situations, people are uncomfortable discussing risks. Bringing up potential failures puts people on edge, and some might want to deny that such a problem could ever exist or happen.

## **Details:**

The [U.S. Environmental Protection Agency](#) has identified seven “rules” for effective risk assessment and management. These rules are:

1. Problem formulation
2. Stakeholder involvement
3. Quantitative risk assessment
4. Communication
5. Iteration and evaluation
6. Informed decision making
7. Flexibility

## **RSS**

### **Definition**

RSS stands for Rich Site Summary or Really Simple Syndication and is a XML message format for syndicating blog, news and other Web content. RSS has also been used to refer to RDF Site Summary, the first version of RSS. Essentially, all three terms are versions of the same technology.

RSS is often used to generically refer to all forms of Web feeds, including the competing standard, Atom.

RSS feeds offer users privacy, convenience and the ability to filter and search content. Feeds are read using news aggregators, which can either be a standalone application or Web-based tool. By subscribing to feeds, users can easily skim information from multiple sites and blogs without visiting the individual sites or sign up for e-mail newsletters.

### **Business applications**

The obvious benefit of RSS to business is the technology gives companies another way to keep in touch with customers and readers. By offering feeds to public content, businesses do not have to incur the costs of e-mail campaigns to push content to readers or risk that costumers will “forget” their Web sites. On the other hand, they also may lose the contact data and information gleaned from Web site visits.

RSS is outgrowing its consumer roots as companies and vendors explore how the potential business applications for RSS. Dana Gardner, a principal analyst of Interarbor Solutions and ZDNet blogger, [noted in 2007](#) that enterprises were exploring the use of custom feeds as a way to promote in-house content.

One obvious use is to syndicate internal content within the organization, an application that might be able to revitalize corporate intranets, as IT Business Edge Blogger Ann All [pointed out](#). Businesses are using RSS feeds to monitor data warehouse quality, streamline document management and communicate with business partners.

During the past two years, niche vendors have begun to use RSS in [mashups to offer business products](#), including solutions that allow business users to perform basic data integration. Gardner calls these vendors “feed bleed providers” and lists that Apatar, JackBe and [StrikeIron](#) as vendors who offer tools for “mashing up” and presenting on-site content.

David Lavenda, vice president of marketing and product strategy at [WorkLight](#), which provides enterprise-class Web 2.0 solutions, explained in [this IT Business Edge interview](#) how a business user might use RSS feeds to share templates to distribute documents as well as information.

## **Security Issues**

Some have expressed concern about the security of RSS feeds. These concerns have been hypothetical and little has been written on the topic in recent years. In 2005, Greg Reinacker, the founder and CTO of NewsGator Technologies, [argued](#) there is no need for additional RSS-specific protocols, since RSS is transported by HTTP and the same security protocols.

Reinacker [also noted](#), however, that there are security best practices that news aggregators should follow.

## **Technical Notes**

RSS was first developed and introduced by NetScape in 1999, although similar ideas had been tried before this. The specifications have been under the Creative Commons license since 2003, thanks to Harvard, which acquired them after a series of unusual events outlined on [Harvard Law's Web site](#). RSS files must conform to the XML 1.0 specification, as published on the [World Wide Web Consortium Web site](#).

Creating feeds is a pretty simple process for IT divisions, requiring a server connected to the Internet for storing the feeds, a database describing the content, and a server-side scripting language with access to your database.

There are enterprise RSS solutions you can buy. For instance, NewsGator, Attensa and KnowNow are known for their enterprise [RSS products](#). In addition to filtering, collaboration and access control, enterprise RSS solutions typically support integration with other systems and run behind the firewall. As Web 2.0 tools such as blogging and social networking enter the

workplace, [RSS enterprise solutions](#) could be absorbed and integrated into content management suites.

## SaaS

### Definition

SaaS stands for [software as a service](#) and basically means that a software vendor provides a business with licenses for an application to be used on demand for a specified time period. The customer may download the application to his or her own servers or computers or the software vendor can host the application. Either way, the application is generally available for use by the customer as needed until the end of the specified contract date.

Applications offered via SaaS allow more than one customer to use a shared data model, which is different than the application service provider (ASP) products. Also, software vendors who offer SaaS achieve greater efficiencies in the deployment and management of such software.

Software vendors provided on-demand products long before the term “software as a service” was coined. As early as 1999, companies were able to use applications in this way; however, in late 2000, the term had become popular and the acronym “SaaS” followed in 2001.

### Business Applications

SaaS allows businesses to gain rights to applications and software for use without the [costly need to purchase licenses](#) for every device. Customers pay for each application on a per-user basis. This also allows [small and medium sized companies](#) to provide users with the same applications and tools that the larger businesses use.

Also, business users of SaaS applications do not need to download patches or upgrades to the software because the software vendor centrally performs such updates. This is attractive to many smaller businesses, because fewer internal IT staff are required to manage applications and upgrades for end-users.

But companies and enterprises of all sizes have begun embracing SaaS. Reports in 2009 have shown that nearly one third of retail companies use a form of [SaaS for Web commerce](#).

### Concerns

One of the [main concerns](#) about using SaaS is that since the applications are generally Web accessible, if Internet connectivity goes down, users cannot access the software. However, reliable Internet connectivity is more the norm these days, so many companies do not fear possible downtime with SaaS implementations.

Another concern with SaaS, though, is security. Companies such as [Trend Micro](#) and [McAfee](#) have begun to offer “security as a service” products to help companies provide the service in a more [secure environment](#).

Other issues with SaaS involve implementation problems. In many organizations, SaaS may be implemented without the involvement or help of the IT staff. Also, system upgrades, API changes, and SaaS updates can all [affect the SaaS implementation](#), and sometimes the cause of problems can be difficult to pinpoint.

## Technical Details

When implementing [SaaS architectures](#), each can be classified in one of the following four levels:

- **Level 1**—Ad-Hoc Custom where each customer hosts its own version of the application.
- **Level 2**—Configurable level provides flexibility via configurable metadata.
- **Level 3**—Configurable, Multi-Tenant-Efficiency provides a single program to serve all customers.
- **Level 4**—Scalable, Configurable, Multi-Tenant-Efficiency provides a multitier architecture to allow for scalability among servers.

## Sarbanes-Oxley

### Definition

The [Sarbanes-Oxley Act of 2002](#) (Public Company Accounting Reform and Investor Protection Act of 2002 Pub. L. No. 107-204, 116 Stat. 745) is a United States Federal law originating from Senator Paul Sarbanes, a democrat from Maryland, and Representative Michael G. Oxley, a republican from Ohio. The law was created in reaction to major corporate accounting scandals, such as those dealing with Enron, Tyco International, Adelphia, and WorldCom. Abuses of corporate power within these companies cost investors and employees billions of dollars, collapsed the affected companies, and radically affected the U.S. stock market.

### Business Impact

The law created new and improved rules for all U.S. public company boards, management, and public accounting firms, however; the law does not encompass privately held companies. The act contains 11 titles that spells out additional corporate board responsibilities, defines criminal penalties that can be enforced, and requires the SEC (Securities and Exchange Commission) to police and judge on the specifications of the new law.

### Concerns

Even after it has been in place for several years, there is still some debate over this law. Sections are designed to be interpreted by the SEC, and the [benefits of the law have yet to show themselves](#) in protecting the public or even corporations from themselves. Since this is still fairly new, there have yet to be trials based upon the law to build a foundation of bounds. Also, many companies have even built entire departments to deal with compliance, which means the companies have spent large amounts of money just to ensure they are staying within the law.

These additional costs put the American companies at a disadvantage against foreign competitors.

### **Further information**

The law also created a public/government agency, the [Public Company Accounting Oversight Board](#) (PCAOB), which has been charged with oversight, inspection, disciplining and auditing of public companies. The law has also increased required external accounting audits, corporate governance, internal controls, and transparent financial disclosure. In return, IT departments must keep more backups and archives of data, which has led to the need for greater resources to support these additional financial applications.

## **Security Appliances**

### **Definition**

A security appliance is a low-cost computer system designed to provide specialized security functions, such as a network firewall or e-mail security. The appliance is a [hardware component that includes all the required software](#), including a proprietary operating system. Like household appliances, security appliances usually cannot be repaired or upgraded by the administrator, and they are usually “plug and play,” meaning they simply need to be plugged into the network to work.

### **Business applications**

Security appliances offer specialized security functions in a single, pre-configured, easy-to-manage and -deploy form factor. Organizations can deploy these “point solutions” to enforce policies, detect network intrusions, create and manage virtual private networks, manage e-mail security, and more.

### **Deployment Concerns**

Security appliances are intended to simplify security, but some [appliances have evolved](#) to such an extent that they provide a simple way to manage complexity. This is the case with appliances for application integration, which is inherently complex.

Organizations increasingly rely on appliances of all types, resulting in “[appliance overload](#).” As organizations deploy more and more appliances to perform security and other functions, the ease-of-use and management benefits are replaced by complexity and the cost of managing multiple single-point solutions.

## **Security Metrics**

### **Definition**

Security metrics are measurements of key performance indicators that [help organizations establish relationships](#) between different dimensions of their security strategy.

## **Business applications**

Security metrics are often used to [justify security spending](#) to C-level executives, whether by illustrating the present risk or showing how security investments have helped mitigate risk. For example, an organization might measure the number of incidents that occurred within an IT infrastructure during a given time period, and the amount of time and money needed to resolve them. This data may help the organization demonstrate a need for additional security spending or prove a return on technology investment.

## **Deployment Concerns**

Given the dynamic nature of technology and the threat landscape, [security metrics quickly become outdated](#). They also lack standardization, so organizations cannot easily compare their security posture to best practices or even other organizations within the same industry. Organizations can deploy an automated security metrics program to help ensure that metrics are current, but they are still limited in their ability to compare metrics.

When presenting security metrics, IT professionals must be careful to present the findings in [relation to the business](#). C-level executives and upper-management must be able to understand the business impact of the security metrics to understand how they justify security spending.

## **Service Level Agreement**

### **Definition**

The Service Level Agreement (SLA) is the section of an overall service agreement between two entities for the level of performance or delivery times to be maintained during the length of the contract. The two entities are usually known as the service provider and the customer, and can involve legal agreements where monies are involved or more informal contracts among [internal business units](#).

An SLA is usually comprised of many sections that define the parties' responsibilities, how the service is to be performed and guarantees or warranties that are part of the agreement. Each service has a [level of expectation](#) that is agreed upon, but within the SLA there may be levels of availability, serviceability, performance, operation or other levels specific to the service itself. Also, the SLA will define the ideal target level as well as an acceptable minimum

### **Business Applications**

By knowing the expected level of service as well as the minimum level, the customer can then use that service to its maximum. This is also very helpful if the customer is an intermediary, who resells or bundles the service into a larger service that is being sold. SLAs have been in use since the early 1980's by landline telephone companies with their larger corporate customers and

resellers of their service. The concept caught on, and other businesses and business units in larger companies began to use the terminology and ideals setup in those early telecommunication service contracts.

The idea of creating a larger service from smaller services almost requires SLAs from the upstream service providers. For example, to have [nationwide cell phone coverage](#), you would not need to build towers and antennas all across the country. Instead you could find local and regional companies that offer the same service, write up an SLA and measure the results. Then to your customers, you offer a similar SLA. In the event the original SLA is not met by the company from which you are purchasing, you can still control your costs when your customers abide by the SLA you have with them. This gives a company the ability to use many [sub contractors to provide](#) the greater service, yet control the costs and resources to offer larger products.

## Concerns

With efficiency comes the possibility of corruption. When using the ideals set forth in IT service management, applying metrics to the process and guaranteeing delivery times is very good for management of manufacturing products. But when you apply this methodology to the call center, coding, or system design, [reliability and creativity fade to the back](#) in order to meet the SLA, and thus a company no longer provides the best service to the end customer. By giving a defined, specific metric, delivering that exact idea becomes the goal, and often teams are forced to engineer to meet the deadline, not give the best possible product.

## Technical Details

The use of SLAs has become widespread with the use of IT service management foundations such as itSMF or ITIL. A common use in IT service management is the service desk also known as a call center. [Metrics in these cases are commonly](#) identified as:

- ABA (Abandonment Average): A percentage of inbound call hang-ups while waiting to be answered.
- ASA (Average Speed to Answer): An average number of seconds it takes for a call to be answered by the service center.
- TSF (Time Service Factor): A percentage of calls answered within a time frame, a good example is saying 80% in 20 seconds.
- FCR (First Call Resolution): A percentage of incoming calls that can be solved without the use of a service desk person calling back or without having the customer call back to finish the case.
- TAT (Turn Around Time): Time taken to complete a certain job.

These metrics are recorded and monitored to provide feedback to management on the efficiency and usefulness of the call center personnel and to help indicate where training or more resources are needed.



The use of SLAs is not limited to the world of IT or telecommunications--they are also used in real estate, medical and any field that provides a product or service to a customer. Service oriented people and businesses have a need to measure and hold themselves accountable, and SLAs provide the metrics and ideals for entities to agree upon.

## Six Sigma

### Definition

[Six Sigma](#) is used in a form of statistics known as [process capability](#) studies. Processes and procedures that operate within the term "Six Sigma quality" over the short term are assumed to produce long-term defect levels below 3.4 defects per million opportunities ([DPMO](#)). Six Sigma's main goal is to improve all procedures and processes to eliminate errors in manufacturing.

### Business applications

By utilizing Six Sigma and lean Six Sigma ideas to eliminate waste in a process, a business can (in theory) reduce their costs and increase capacity for their existing products and services. [Motorola](#) was the initial implementer of the Six Sigma ideals. They saw huge savings and a reduction in manufacturing problems after implementation. Honeywell and [General Electric](#) followed with implementing Six Sigma methodologies in their processes as well, to great success.

### Controversies

Quality expert Joseph M. Juran has described Six Sigma as, "A basic version of quality improvement." He said, "There is nothing new there. It includes what we used to call facilitators. They've adopted more flamboyant terms, like belts with different colors. I think that concept has merit to set apart, to create specialists who can be very helpful. Again, that's not a new idea. The American Society for Quality long ago established certificates, such as for reliability engineers."

According to [this article](#), "... of 58 large companies that have announced Six Sigma programs, 91 percent have trailed the S&P 500 since, according to an analysis by Charles Holland of consulting firm Qualpro (which espouses a competing quality-improvement process)."

Among other concerns, the Six Sigma methods do not translate well to all types of manufacturing. For example, having 3.4 DPMO might be a good rate for manufacturing dishwashers; however, the same rate would need to be much lower for medical devices—it could mean life or death for the user.

### Technical details

The following is a [list of the short-term sigma levels](#) as they correspond to long-term DPMO values:

1 sigma = 690,000 DPMO = 31% efficiency  
2 sigma = 308,000 DPMO = 69.2% efficiency  
3 sigma = 66,800 DPMO = 93.32% efficiency  
4 sigma = 6,210 DPMO = 99.379% efficiency  
5 sigma = 230 DPMO = 99.977% efficiency  
6 sigma = 3.4 DPMO = 99.9997% efficiency

## Smart Grid

### Definition

A "[smart grid](#)" is a modernized, bi-directional, electricity delivery system that regulates energy consumers' usage, whether residential, commercial or industrial, by controlling appliances and other devices. The goal of a smart grid is to reduce energy consumption (and therefore demand), save money and increase reliability. Governments also promote upgrading to smart grids as a way to achieve energy independence and fight global warming.

A smart grid can include:

- A monitoring system that tracks all energy flowing through the system
- Transmission lines that reduce power loss
- Integration capability for alternative energy sources (e.g., wind, solar)

Smart meters are probably the most widely known parts of a smart grid system. A smart meter is a technologically advanced meter that provides more detail about energy consumption than conventional meters. These meters are generally capable of transmitting usage information back to the providing utility for monitoring and billing purposes. Smart meter manufacturers and networking/communications providers include Trilliant, SmartSynch, Alliant and [Itron, Inc.](#), the market share top-spot holder in North America and worldwide.

Although primarily used to monitor and regulate electricity distribution and usage, smart meters are increasingly providing the same function for water and natural gas consumption.

### Business applications

Smart grids offer energy consumers the opportunity to identify the main sources of energy consumption and quantify energy use. From this information, users can take steps to reduce consumption, saving money and energy. Based on the information obtained from items like smart meters, consumers can replace energy-inefficient items such as appliances, electronic devices, HVAC equipment and light bulbs with more efficient alternatives. Other demand-reduction steps on the supply side include controlling consumption at the appliance or systems

level by incorporating measures that switch off heavy-consumption devices during peak hours so that they operate during low-demand times of the day.

Overall, smart grids put more responsibility for energy consumption in the hands of the consumer by providing feedback about specific use. Electricity providers receive information about transmission losses that enable them to eliminate wastefulness in infrastructure. The net result is energy use reduction and conservation by way of an informed, empowered consumer base and an efficient, intelligent electricity distribution system. As the U.S. Department of Energy put it in its statement regarding [smart grid stimulus awards](#):

“Modernizing the grid will [create tens of thousands of jobs](#), save money for consumers and businesses, and allow for the transportation of renewable energy across the nation.”

## **Obstacles**

The biggest obstacles to large-scale implementation of smart grid technology are cost of transition and lack of public awareness of benefit. Additionally, a few highly publicized glitches in billing from smart meter providers PG&E in California and [CenterPoint](#) in Texas and [privacy concerns have deepened wariness](#), creating suspicion that such programs are simply another way to obfuscate already complex billing processes and further erode privacy.

Legacy systems present a challenge to wider adoption of smart grid tech. Existing infrastructure cannot currently accommodate the new technology and would largely need to be replaced, although a hybridized infrastructure consisting of older, viable components and smart grid tech shows promise as a way to ease the transition and constrain cost. While corporations like GE, [Verizon](#), and [Cisco](#) all have smart grid strategies in various stages of development, transition costs, in conjunction with current economic conditions, have slowed efforts to push smart grid initiatives forward.

In addition, a lack of awareness in the public sector about smart grid benefit potential has significantly impeded growth. Research by Parks Associates indicated that over 40 percent of consumers are unfamiliar with the phrase "smart grid." It seems logical that more people, whether household or corporate consumers, would call for initiatives in their communities if the advantages of smart grid tech over traditional systems were explained in clear terms and made widely known. But, attempts to roll out time-of-use pricing and other related initiatives have been met with reactions ranging from indifference to outright hostility.

However, outreach programs and "cash for energy-guzzler" programs have been moderately successful in educating all consumers, whether in business or in the home, about the personal and global benefits of reducing consumption using this modernized system. With the [U.S. Department of Energy awarding 3.4 billion dollars in smart grid stimulus grants](#) to fund over 100 smart grid projects, [Earth2Tech.com](#) and other smart tech watchers see evidence of the mainstreaming of smart grid tech and predict a large boost in implementation nation-wide.

## SMBs

### Definition

SMB stands for [small and medium-sized businesses](#). In the United States, a company qualifies as a small business when it has less than 100 employees. A medium-sized company would employ fewer than 500 employees.

In the European Union, the term used is small and medium-sized enterprises, and the head-counts are a bit different. Any company with less than 50 employees is considered to be a small company, while an enterprise that employs fewer than 250 workers would be called medium-sized.

According to the [Small Business Administration](#), businesses with fewer than 500 employees employ more than half of all workers in the private sector. These same businesses pay nearly 44 percent of the total private payroll in the United States. This growing segment of U.S. business also accounted for 64 percent of the new jobs created from 1993 through 2008.

### SMB Market

Although SMBs may not employ large numbers of people, many large companies provide business services and equipment just for this important business segment. Companies such as [Hewlett-Packard](#), [Lenovo](#), [Dell](#) and [Cisco](#) have all realized the money to be made in this market and have thus begun offering SMB-specific products.

SMBs also have different business needs than their larger enterprise counterparts. In many ways, [SMBs' technical needs mirror those of consumers](#) because such companies may not buy in larger volumes, probably do not have as large storage or server needs, and have much smaller, [tighter budgets](#).

That being said, many market experts believe that unlike larger corporations, [SMBs would not make deep cuts to their IT spending budgets](#) during the recession. Also, the U.S. Small Business Administration charges SMBs with the task of [leading the country out of the recession](#) through efficiencies created via technology that enable such companies to maximize profits during the down economy.

### Business Concerns for SMBs

Some of the same issues that plague large enterprises are also big concerns for SMBs. According to the [2009 SMB Insights Report from Microsoft](#), key issues for SMBs in the coming year will most likely be IT investments, [cost containment](#), [customer retention](#), [cloud-computing](#) solutions, and partnerships with [value-added resellers](#) (VARs).

Other issues that SMBs should be concerned with, but may not identify as a top priority include security and disaster recovery. In the case of IT security, experts believe that hackers may target SMBs for attacks because they believe that such smaller entities are easier targets. To proactively prevent such attacks, [SMBs should consider creating a multi-layered security strategy](#) that includes not only antivirus software and anti-spyware programs, but also firewalls.

Effective [security policies](#) should be created, explained, and enforced with all employees. Workers who use computers and the Internet should be knowledgeable on how to create and use effective passwords and how to identify and avoid possible malicious e-mail and websites.

Also, SMBs must have a plan for [disaster recovery](#) and [business continuity](#). In the event of a major disaster, a company should know that its data is secure and that a process is in place for getting the business back up and running in an acceptable amount of time—without losing money or customers.

## **Technology and SMBs**

Although it was previously believed that SMBs held back on adopting new technology until enterprises proved it to be worth the investment, in recent months, studies have shown that large numbers of SMBs have become the first adopters of [software-as-a-service](#) (SaaS). Also, SMBs have identified [green technologies](#) as a priority to their businesses.

As mentioned previously, many technological needs of SMBs are similar to consumer solutions. Since [SMBs](#) are supplying IT to a smaller group of workers, they often gravitate toward items that can be purchased on a smaller scale.

## **SOA**

### **Definition**

SOA (So-Ah) stands for service-oriented architecture. It is a design approach and philosophy – “architecture” -- for systems and applications. SOA is generally seen as evolving out of distributed computing and modular programming methods, such as object-oriented programming.

### **Business applications**

There are a number of reasons why companies might move to a service-oriented architecture. The most common reasons are to:

**Reuse or share business processes as services.** To simplify, services are collections of code that do something. This business processes - such as run a credit card payment or billing a client – can be “packaged” as a service. Those services then can share or reuse that service either internally or with external partners, generally over the Internet.

**Respond more quickly to changing business needs.** Since business processes can be packaged as services, IT can mix and match services as needed to deploy new applications or update existing applications quickly.

**Simplify and reduce integration work.** Most integration work relies on point-to-point integration. This is an inflexible approach that can cause integration to fail if a new system, application or component is added or if any changes are made. Since SOA uses loose coupling, it is said to simplify the integration work and reduce the chance that a connection will fail.

**Integrate legacy systems.** Again, since SOA calls for packaging application functions as services, you can service-enable legacy systems, making it easier to access the data or functions on those systems.

For an example of how an online company, VetSourced, used SOA to further business goals, see [“VetSource’s SOA Success Story.”](#)

## **Controversy**

For architecture, SOA has had its fair share of controversy. Some question whether SOA is actually anything new or just a glorified version of modular programming.

There is also the unresolved question of how many SOAs are successful. Burton Group analyst Anne Thomas Manes (see [“Looking for SOA Success Stories”](#)) noted she had a difficult time finding true SOA success stories in early 2008 and, more recently, [Gartner reported](#) its research found interest and investment in SOA were declining. There are also unresolved questions about how to calculate SOA's return on investment. (See [“Execs Have a ROI Issue with SOA”](#) and [“Incremental Approach Can Help Ease SOA Pain”](#)) That might be making organizations unsure of SOA's value.

Defining whether or SOA is successful is further complicated by the debate over what qualifies as an SOA and what does not. Despite disagreements over the nuances of defining SOA, there are some widely agreed upon characteristics that make SOA unique.

For instance, Gartner defines the SOA style as having five qualities: modular (these modular pieces are referred to as services), distributable, describable, sharable and loosely coupled. These last two items – sharable, sometimes called reusable, and loosely coupled - are generally cited as the key difference between SOA and other styles of system design.

Another SOA-related controversy is that vendors have labeled products as SOA, causing some in the industry to fear companies will be misled and believe they are “buying” SOA.

## **Technical details**

SOA itself is not tied to a particular language, middleware, interface or other technology component. That said, there are many supporting technologies that can help with SOA deployments, including SOA governance tools, registry/repositories and enterprise service buses.

## Solaris

### Definition

Solaris is an operating system developed by Sun Microsystems. It is often referred to as SunOS 5.x, and is based on the AT&T UNIX System V R4. It is a UNIX operating system that encompasses both servers and desktop systems.

[SunOS](#) is based on BSD initially written by Bill Joy, the founder of Sun Microsystems, who released the first public version of SunOS in 1983. The last version of SunOS was released in 1993. With Solaris, the kernel is based on AT&T UNIX V R4, and not BSD.

### Business Applications

Solaris is used for web, application, and database server applications. JAVA got its origin with Solaris, and the modern day Solaris operating system offers many development and debugging tools to the JAVA developer.

Companies such as Oracle choose Solaris as their prime development platform for high-speed transactions and reliability. [Solaris is qualified](#) for Oracle Application server, and Oracle transactional database, including the ability to form large clusters in a GRID environment for unlimited scaling.

With [security being the forefront](#) of all enterprises today, Solaris offers “grade A” security out of the box. Sun has made the system secure from the installation--you must activate services you need during configuration, which allows for finer control over the security you need for your systems. This is why many [enterprises choose Solaris](#) as their application and web server OS.

### Deployment Concerns

Since Solaris is a UNIX-based system, it requires a highly skilled administrator to manage the system. Patching the operating system for issues and problems can become quite complex depending on which applications are deployed on the system. Also, [Sun Microsystems](#) is a fast paced company. Each Solaris version is supported for 10 years after its release and it seems that the number patches available from Sun are overwhelming in comparison to other UNIX-based systems.

### Technical details

The current version, Solaris 10, operates on both the Sun SPARC and Intel or AMD x86 series processors. There are [two types](#) of Solaris, Solaris and OpenSolaris. Solaris is a fully supported and purchased product from Sun, while OpenSolaris is the bleeding edge open-source community version; however, Sun does promote early fixes and technology to OpenSolaris before those fixes are made available to Solaris.



Solaris is a 64-bit operating system that is very scalable in order to handle very large databases and applications. The [SPARC](#) (Scalable Processor Architecture) chip that Solaris uses as its primary platform is designed to deliver the speed and reliability that enterprise environments require.

Solaris also offers the new ZFS file system that is now regarded as one of the most innovative file systems in an OS. [With ZFS](#) you get the capabilities of a SAN disk array-- such as snapshots, cloning and RAID striping—all within the operating system. The highlight is that with auto corruption scanning, your data will never be corrupt.

## Standards Bodies

### Definition

A [standards body](#) is an entity whose primary job is to develop, amend and maintain standards that direct the interests of people or industry. Standards bodies are classified by their role and their regional, local, national, or global influence. Generally, the standards group will not contain anyone associated with the organization for which they are creating the standards.

### Business applications

It is essential to develop clear standards when creating new technologies—you need a baseline set of rules upon which the technology will be used and developed. Having an agreed [set standards](#) prior to developing a product can help improve the quality of your product, ensure that your product works with other products, and provide guidelines for research and development of future products. Also, when a standards body creates a set of standards and they are widely accepted by other companies, they can become de facto standards for that industry.

### Concerns

Companies sometimes feel the need to review the bodies from which they receive standards policies. In the [case of IBM](#), the company felt that some standards bodies function without much openness about their practices, and so IBM will review the many standards organizations they currently work with, and will most likely withdraw from some of the organizations.

## Structured Data Integration

### Definition

Structured data describes data that is organized and stored in a defined format. A list of these defined formats, or data structure types, is maintained on the [National Institute of Standards & Technology Web site](#).



The opposite of structured data is unstructured data, which includes text and rich media files. In recent years, analysts and vendors have begun to recognize identify a third type of data – semi-structured data, which includes more official Word documents, spreadsheets and other office suite documents.

### **Business applications and concerns**

The big benefit of structured data is that you can run queries or reports against the data using a data-management system.

The problem is, structured data has proliferated substantially over the years, a situation that has created a number of problems for organizations. First, there's no one system that can store all this data, so organizations have had to spend more adding, running and maintaining databases and data warehouses. This has led to data siloes, so to query the data, organizations have been forced to invest in data integration.

Managing structured data has become very complicated. But as difficult as structured data may be, it's a small problem compared to the challenge of unstructured data. One much-cited statistic is that 80 percent of all enterprise information is stored as unstructured data.

The new information management challenge facing organizations is [how to integrate their repositories of structured data with the unstructured data](#) stored haphazardly throughout their networks.

### **Technical Notes**

Though information stored in databases and data management systems is structured data, it's the data format itself – and not where it's stored – that defines structured data. As this [TechTarget article](#) explained, “There is no way to store anything not defined in the data model, and everything defined in the data model must have a value (even if it's only some sort of "VALUE ABSENT" flag).”

Another characteristic of structured data is the individual data points do not have meaning as a stand-alone data point. Instead, meaning is derived from the relationship between the data items in the file. TechWorld explained it this way: “A time and date (whether stored in binary or text form) has no meaning in itself, the importance lies in relating it to a particular phone call made at that time. Without the context, the web of relationships to other data items, an individual data item is meaningless.”

Spreadsheets may appear to the general user to be structured data, but actually they are considered unstructured data because the application does not enforced or impose relationship between the data. In most cases, the information is actually just text. Some people now refer to [this type of document](#) as “semi-structured” because it falls somewhere in between the randomness of text and the rigid format of structured data.

# Twitter

## Definition

[Twitter](#) is a service that allows users to post micro-blogs, known as “tweets,” which can be read by other users who “follow” by subscribing to a user’s profile. Each tweet is actually a text-based post up to 140 characters long. Twitter users send and receive tweets in several ways: via SMS, from the Twitter website, or via instant message. The [Twitter service](#) was first introduced in 2006 and is free to use.

## Business applications

Twitter is mainly a social networking site, meaning it was created to bring together people who share like activities and interests. However, various organizations have used the technology for other purposes.

The Los Angeles Fire Department used Twitter to communicate during the 2007 California wildfires. NASA has used Twitter to provide updates during Space Shuttle missions. President Barack Obama used Twitter during his 2008 presidential campaign. Israel was the first government to use Twitter to take questions during a worldwide press conference concerning the war against Hamas in Gaza.

Considering these various uses of the technology, there could be other ways to harness the micro-blogging service for use in the business world.

## Concerns

With so many ways to keep in contact with friends, Twitter users often feel “too connected” since users can send and receive messages at all hours of the day, and some users feel the need to post about every activity from breakfast through bedtime rituals. Also, if users tweet via SMS messages, there are cell phone charges to consider. But most users find the most challenge in attempting to publish their thoughts within the limited text constraints.

There are also issues with scammers who are targeting Twitter users with [phishing scams](#). A scammer might send out a tweet with a link to a page that looks like the Twitter page, but is actually a fake page to try to steal the user’s login and password.

## Technical details

Twitter uses the Ruby on Rails open-source web application framework. The messages are handled with a persistent queue server written with the Scala programming language.

## Ultra-Wide Band

### Definition

Ultra-wide band is a means of transmitting data at speeds of 480 Megabits per second using low power in a wireless personal-area network (PAN). The bottom line is that there are several technologies, such as Bluetooth and 802.11n that do many of the things for which UWB was originally aimed at.

After a long and frustrating process that failed to produce an IEEE standard, the WiMedia Alliance has emerged as the key UWB consortium. The group consists of more than 350 companies including Alereon, CSR, Intel, Nokia, NXP, Samsung Electronics, Staccato Communications, Stonestreet One and Wisair. Recent news about the technology has not been good. For instance, last autumn UWB vendor WiQuest closed down. This led to speculation that the technology was dead.

### Prospects

The gloom is not universal, however. There have been some recent signs that UWB is making a comeback as a means to distribute high definition and other demanding signals in home networks. There are reports that Sony is pushing a UWB technology it calls TransferJet as a way to link cameras into networks. At CES, a company named Tzero demonstrated HDMI multimedia streaming using UWB. Reports say that the technology delivers content at the UWB speed of 480 Mbps over 20 meters.

UWB appears to have limited application for business. Of course, it can have an impact in its role a wireless USB enabler. UWB can ferry signals in a small office/home office and for niche applications such as trading electronic business card information at shows.

### Implementations

There also has been some recent news. For instance, in January, ShopperTrak extended its employee locator service to include UWB functionality. The real time locating system (RTLS) is aimed at helping store personnel find the best possible position to help shoppers. Its FloorTrak enhancement features UWB badges from Time Domain that enables other elements of the system such as heat sensors and video cameras to more effectively distinguish between store personnel and customers. Despite these utilizations, it seems that UWB has found limited success in commercial applications.

## Unified Communications

### Definition

Unified communications is the linking of communications applications within business processes. It features the ability to reach any devices on any network and includes a presence element that lets parties know who is available and unavailable on each device.

UC has a great number of business applications, from conferencing of widely dispersed groups using different tools to contact center personnel. The keys are that UC makes workforces more efficient and cuts total cost and complexity of the communications infrastructure. When used to interact with customers or prospects, UC services can increase satisfaction and lead to more sales or solve problems that threaten to make customers leave. For instance, suppose a customer service representative senses interest on the part of a client in a product about which he has limited knowledge. That CSR can use UC to identify the internal person with the requisite knowledge of the product and connect them to the prospect immediately. This, of course, is far more likely to end in a sale than taking a message and having the expert call back later.

UC is a collection of pre-existing technologies that are linked together in an innovative web. The underpinning is IP over wired and wireless networks. Beyond that, the technical details vary depending on the precise nature of the UC application. Common UC applications are instant messaging, short message services, VoIP and video conferencing. The thread is the provisioning of presence capabilities. UC relies upon the Session Initiation Protocol (SIP) for establishment and teardown of calls and for other vital connectivity functions.

### **Slow Acceptance for UC**

Despite all its advantages, UC has been slow to take off. It is a significant undertaking and may not be at the top or an organization's priority list. UC also has been confused with unified messaging – which is the concentration and delivery of messages to one repository. UC also is a hard sell because it largely involves applications the organization already uses. The advantages, therefore, are not as readily apparent as if the applications were not already being used.

## **Unified Threat Management**

### **Definition**

Unified threat management describes technology that consolidates traditionally disparate security functions in one device. Unified threat management (UTM) devices typically include a network firewall, virtual private networks, antivirus and content filtering. By integrating these technologies, UTM devices offer protection against multiple threats for less than it would cost an organization to deploy separate firewall, VPN, antivirus and content-filtering appliances. UTM devices also offer simplified deployment, ease of use and [more exacting management](#).

### **Business applications**

Unified threat management devices are commonly deployed by SMBs and remote branches, which benefit from a reduction in the number of [stand-alone security appliances](#) they have to manage as well as the number of vendors they have to deal with. UTM devices also offer more robust [security coverage](#) for the same reason. Because the various functions of a UTM device are

integrated by a single vendor, they should provide more comprehensive coverage than multiple standalone appliances.

## **Deployment concerns**

Organizations that choose to deploy a UTM device may be forced to pay for unneeded functions, as it's unlikely that warranties and subscriptions for all of the organization's security point solutions will be due at the same time. Experts suggest turning on functions as its needed.

While UTM devices are beneficial for resource-strapped SMBs, they have not demonstrated the [performance and integration maturity](#) required for enterprise deployment. They require organizations to give up a best-of-breed approach to security and represent a single point of failure.

## **Technical details**

Manufacturers are increasingly adding functions to their unified threat management devices, including WAN load balancing, virtual LANs, HTTPS inspection, and VoIP security. These devices have been dubbed [extensible threat management \(XTM\)](#) devices.

## **Unstructured Data Integration**

### **Definition**

Unstructured data refers to data stored as text or rich media (bitmap) objects.

The opposite of unstructured data is structured data, although more recently, some analysts have begun to identify a third type of data: semi-structured data, which include more official Word documents, spreadsheets and other office suite documents.

### **Business applications and concerns**

Eighty percent of all enterprise information is stored as unstructured data. Given that e-mail, Web logs, call center records, Word documents and spreadsheets are all "unstructured data," it's easy to see how executives and managers would benefit from being able to reliably access and query this information.

[A 2008 report by the Aberdeen Group](#) showed best-in-class companies who integrate unstructured data reported:

1. Better response time to customer demand.
2. Improved employee productivity.
3. Reduced risks of harmful events.
4. Better insight into customers than their counterparts.

Best-in-class companies also reported that reducing risks by preventing harmful events and increasing employee productivity were the top drivers for pursuing integration of unstructured data.

In recent years, regulatory compliance and data-security issues have forced many companies to act on the problem of unstructured data.

The big challenge with unstructured data is to integrate it with more formal, structured data. For instance, very [little unstructured data can be accessed by existing business intelligence](#) tools. If BI tools could draw from both types of data, leaders would gain better insight into the business.

## **Deployment Options**

There are a range of options for finding, storing and accessing unstructured data. Enterprise search tools, enterprise content-management systems, text mining and analytic tools and intranets are among the solutions companies use to organize unstructured data.

BPM tools have also been used to “bridge the gap” between structured and unstructured data. Geoffrey Weglarz, a veteran of relational database technologies, multidimensional database technologies and linguistics, pointed out three specific situations where BPM had been used to marry unstructured data with structured data in [this 2004 DM Review](#).

In the past two years, text analytics tools have entered the data-integration market. Philip Russom, an analyst for The Data Warehousing Institute, [explained in this IT Business Edge interview](#), that these solutions can analyze natural language and mine it for data that can be imported into database records. Pureplay vendors include [Attensity](#), [ClearForest](#), [Clarabridge](#). Some search tools also include text analytic capabilities, including [Inxight](#), [FAST](#) and [Endeca](#).

Colin White, the founder of BI Research, wrote in 2008 that the three main tools for integrating structured data - data federation, data consolidation and data propagation – could also be applied to unstructured data. Unstructured data would require an additional step of transforming the necessary business information into a semi-structured format, such as XML, or a structured format. He explained the challenges to this approach and outlined possible solutions in [this bEye Network article](#).

## **Emerging Solutions**

There also is an emerging discipline –information management - devoted to the problem of integrating structured and unstructured data. [A Computer Weekly article](#) examined this emerging field, as well as existing integration options and solutions on the horizon.

Another emerging option is [the use of semantic technologies to integrate unstructured data](#).

## **UNIX**

### **Definition**

In [1965](#), a group of AT&T employees at Bell Labs began working on a new multi-tasking operating system that they later called UNIX. It was first available to the public in 1975 after having been rewritten in the C programming language. The name UNIX is a designation given by the open group to an operating system that meets a set of standards based on X/Open Company's XPG4, IEEE's POSIX Standards and ISO C. Today, they are grouped together into a single standard maintained by the [Open Group](#).

## **Business applications**

UNIX is most often used as an operating system for servers that require high input and output of data, usually multi-user systems such as databases and web servers. Version 10 of the MacOS (OSX) desktop platform, however, has met and been [approved](#) as a version of UNIX by the Open Group. The major factor in using UNIX systems is the reliability that comes with the open standards and design methodologies of it. It is slow changing, which provides a [more stable system](#).

## **Concerns**

UNIX is a designation, not a brand. As such, there are many flavors of UNIX, such as Hewlett Packard's HPUNIX, Sun Microsystems' Solaris and IBM's AIX. Though, one of the most widely used operating systems, Linux, does not carry the UNIX certification--even though it meets the technical requirements. Even so, there are those in the industry that try to connect UNIX with open source community. While there is a sort of link, more common than not, the software deployed with UNIX systems is in supported vendor provided applications. This sometimes causes confusion with among those who are not educated in the ways of UNIX.

There have also been recent rumors of [Linux putting UNIX out of play](#), but that seems unlikely for now.

## **Technical details**

UNIX is a certification given to OSs based on the Open Groups standards of [UNIX95, UNIX98 and UNIX03](#). These certifications are based on long running standards that determine the interoperability of source code and internal operations of the operating system. There is a very strict process for attaining the UNIX designation. This [test suite](#) usually involves internationalization and the ability to compile certain machine source code into executable form.

## **Vishing**

### **Definition**

Vishing is VoIP phishing, or the use of VoIP as a social engineering platform aimed at stealing vital information from people.

To date, VoIP has been relatively safe from the viruses and other purely electronic problems that are common in many data networks. These vulnerabilities still exist and will possibly create

problems for VoIP in the future. However, today the most dangerous element of VoIP is the underworld's use of these platforms to steal personal information such as credit card and Social Security numbers.

Thieves like VoIP more than traditional circuit switched telephone networks for such attacks because the platforms offer anonymity. In the traditional setting, a number is terminated to a location. VoIP uses Internet addresses, so the caller can be anywhere. This makes it easier for thieves to quickly set up and tear down scams and, consequently, makes it more difficult for law enforcement people to find them.

### **Caller ID Spoofing**

One approach that vishers use – and one that does have a technical element – is caller ID spoofing. As the name suggests, this is the use of data networking tricks to display a different number on the target's caller ID panel than the actual number from which the call has originated. The fake number may look like it is from the target's bank or insurance company, for instance. This makes it more likely that they will provide the sensitive information.

Vigilance, of course, is the key way in which the problem can be avoided. Such schemes have surfaced recently, and the Better Business Bureau even named this scam as one the top ten for 2008.

It is not hard to see why. In late December 2008, reports surfaced that scammers had attacked vulnerability in an older version of open source provider Asterisk's IP PBX software to make the user's system into a giant auto-dialer. Vendor Digium quickly downloaded a patch to correct the flaw.

## **VoIP**

### **Definition**

Voice over Internet protocol is the use of the Internet protocol (IP) to deliver voice services, often in combination with other applications. While VoIP is mostly associated with the Internet, it can be deployed on any network that uses IP as the basic transmission protocol. For example, a company can link multiple offices throughout the world over a VoIP network that doesn't directly connect to the public Internet.

### **Business Applications**

There are myriad ways in which a business can use VoIP to its advantage. These generally fall into two main groups: VoIP is cheaper, and it is far more flexible than traditional circuit switched telephone services.

Since it uses the Internet, VoIP costs are far less than traditional phone services. This was a particularly big attraction for long distance services. Overall, however, the attractiveness of the low cost of VoIP has somewhat faded. This isn't because it has gotten more expensive. It hasn't.



The reason is that traditional telephone services have cut prices in order to compete. The other reason that cost is less of a prime driver simply is that companies have realized that they must ensure that the services they get are the equal of circuit switched services. Simply, there is a general recognition that voice communications with customers, prospects, partners and co-workers is not the place to save a few bucks.

The good news for VoIP proponents is that the services they offer have gotten far better. Potential customers no longer must make a choice between good services and cheap prices. They can have both, from either circuit switched or VoIP vendors. Indeed, the phone companies increasingly offer VoIP services of their own. This is a Pyrrhic victory for the pure play VoIP providers, since their faith in the technology has been vindicated – but the big cable and phone companies with money, skills and marketing acumen are taking over.

### **Deployment Concerns**

There are a couple of concerns related to VoIP deployment. The fact that a voice call is timing-sensitive is a big challenge. Structural problems in a corporate network that would not impact email or other static classes of content can create big issues for voice calls. On the public Internet, these problems can be even trickier, since they are outside the control of the IT department.

### **Technical Details**

The IP protocol essentially is a way of slicing data, putting each piece into envelopes with destination information and sending them off. Indeed, the postal analogy is a good one: Imagine taking an old fashion tape, slicing it into millions of little pieces, putting each piece into an addressed envelope and mailing them. This essentially is how VoIP works. The challenge is that the Internet protocol is designed to send each envelope over the best route based on conditions at that particular point in time. So one packet (or, in the analogy, one letter) may go from New York to Los Angeles via Cleveland. Another may go via Minnesota and another via Las Vegas. Success is dependent on all the envelopes arriving and the pieces of the tape being successfully taped together in precise fashion. Problems occur when envelopes don't arrive, arrive out of order or not in a uniform cadence. In the world of VoIP calls, the names of these problems are delay, jitter and latency.

## **Vulnerability Assessment**

### **Definition**

Vulnerability assessment is the process of identifying, quantifying and prioritizing the vulnerabilities in a computer, network or communications infrastructure. A vulnerability assessment begins with an inventory of the network or system resources to be assessed. They are

also classified according to their value. Vulnerabilities or potential threats are then identified for the resources, and then mitigated according to their severity and the value of the resource.

## **Business applications**

Businesses conduct vulnerability assessments to determine how secure their network and system resources are and to help determine where to focus their security efforts. There are countless threats and vulnerabilities, but not every one needs to be addressed. That would be impossible. Vulnerability assessment helps prioritize vulnerabilities and the resources they affect so businesses can make informed decisions about how to spend their security dollars.

## **Deployment Concerns**

The tools used for vulnerability assessment are passive in that they typically generate huge reports that are useless unless someone reads them and manually addresses the findings. Doing so can be a daunting task. Even then, it is a cat-and-mouse game. No matter how often an organization conducts a vulnerability assessment, [there is always something to fix](#).

## **Technical details**

There has been some debate as to the viability of vulnerability assessment and its future. Vendors are recognizing the need to provide tools that go beyond simple identification of vulnerabilities to those that [help prevent or fix problems](#) as well. Vendors are also integrating [vulnerability assessment and penetration tools](#) to help users verify the viability of vulnerabilities.

## **WAN Network Protocols**

This article discusses some of the most implemented WAN protocols in enterprise networking environments today.

### **High Level Data Link Control (HDLC)**

HDLC is a Cisco proprietary protocol designed for sending data across serial links. It defines an encapsulation method at the data link layer for transporting data over a public or private network. This protocol is utilized for Leased Line TDM circuits. TDM circuits are probably the oldest circuit types originating from circuit switching technology used by the public switched telephone network that carries your phone traffic. The difference is that companies transporting data traffic require circuit speeds of 256 Kbps to 45 Mbps. That is a data grade circuit which requires equipment at both ends of what is a phone line, for conditioning and formatting the data for those speeds.

The TDM network works with increments called digital signal zero's (DS-0). A DS-0 is a 64 Kbps channel (56 Kbps if in-band signaling used) that is part of the DS-1 industry standard specification. A DS-1 defines a framing standard for transmission across a T1 circuit at 1.544

Mbps with 24 DS-0 channels. A DS-3 defines a framing standard for transmission across a T3 circuit at 44.736 Mbps with 28 DS-1 channels. Some service providers offer what is called Fractional T1 (Frac T1). It is a circuit that runs at a speed less than 1.544 Mbps since it is a subset group of the 24 channels.

The common Fractional T1 speed is 384 Kbps, which is comprised of 6 DS-0 channels. Many router serial interfaces have a feature that split or channelize a T1 circuit. That is useful if you don't want to pay for a full T1 circuit. It does that by differentiating each specific channel from the full T1 circuit. Europe uses somewhat different circuit speed standards called E1 and E3. The E1 circuit is comprised of 30 DS-0 channels and runs at 2.048 Mbps while E3 is comprised of 20 T1 channels and runs at 34.368 Mbps.

### **Digital Subscriber Line (DSL)**

Digital Subscriber Line is a newer broadband technology being utilized for remote dial and access office connectivity. It is very cost effective when compared with ISDN and T1 circuits since it is faster and less expensive. The issue with DSL is that you must be located no more than 18,000 feet from the service provider central office. The demand for high speed Internet access has service providers installing DSL terminating equipment at many central offices. That will increase the chances for availability in your neighborhood if it isn't an option today. The current specification defines three primary technologies, which are Asymmetric DSL (ADSL), Very High Data Rate DSL (VDSL) and Symmetric DSL (SDSL).

### **Asymmetric DSL (ADSL)**

ADSL as the name suggests is asymmetric technology, which allows faster downstream speeds from the service provider to the client than upstream speeds from the client to the service provider. That design matches the flow of Internet and video applications since they typically have the client downloading more information than sending it. Depending on the distance from the service provider central office, downstream speeds can be faster than 6 Mbps and upstream speeds can be as much as 640 Kbps. Being conservative with bridge taps and using increased wire diameter (gauge) will increase traffic rates as well from client to service provider.

The ADSL router or modem at the client will interface with a standard 2 pair telephone line, which is terminated at the service provider DSL Access Multiplexer (DSLAM). At that point the service provider will cross connect their DSLAM with a variety of different equipment such as T1, T3, SONET, Frame Relay, ATM or DSL circuits for transmission across the Internet or to a different central office. As mentioned some clients will utilize ADSL for line sharing their phone calls as well. The DSLAM will split off voice traffic from the data traffic and routed to a Class 5 switch where it is sent across the PSTN using a protocol such as SS7. Many business clients will opt for an additional data line, which is an increased cost however if the voice line isn't available that doesn't affect their Internet connection.

### **Very High Rate DSL (VDSL)**

VDSL is a higher speed DSL specification that will transmit data at distances between 1,000 feet and 4,500 feet across copper telephone lines. Distances of approximately 1000 feet will support speeds of 55 Mbps while distances of 4,500 feet will support an approximate speed of 12 Mbps. There are some technical differences with line encoding however the modem will split off the telephone service as does ADSL for phone calls.

### **Symmetric DSL (SDSL)**

SDSL is somewhat new and as the name suggests transmits data in both directions at T1 speeds. The distance specification from the central office is 21,000 feet and it should be noted that there must be a separate phone line since SDSL won't split off phone traffic. That is currently an issue that is being addressed and should be available this year. SDSL is an always-on service, which reduces the issues with call setup. That and the higher upstream traffic rates make it better suited for web hosting applications since your file downloads sent with downstream traffic is sent with their upstream traffic. There are tremendous opportunities for service providers to sell cost effective high speed Internet access to many clients across the United States today. Telecommuters and business clients can reduce costs with higher speed circuits for sending voice and data from home, access and distribution offices across the Internet.

### **SONET/SDH**

The Synchronous Optical Network (SONET) specification describes a high speed fiber technology used by service providers for transporting voice and data traffic. A SONET network is built with a series of ring segments that are inter-connected. Each SONET segment is comprised of dual counter rotating rings for link diversity should one of the rings be unavailable. The standard OC-1 interface is 51.8 Mbps. The SONET network ring is built with Add/Drop Multiplexers (ADM) which terminate the SONET signal at various metropolitan and national locations. They are Time Division Multiplexers that mux/demux SONET signals from an OC-12 to OC-48 traffic stream. Each ADM has an active and a standby connection to the SONET ring. When a network failure with the active connection is detected, the standby connection is immediately activated. The SONET frame structure is 810 bytes that is comprised of overhead and payload bytes. The overhead is comprised of section and line signaling. The payload bytes are comprised of path signaling and payload. Customer routers such as the Cisco 7507 that support OC-3 interfaces that can interface with an ADM.

### **Dense Wave Division Multiplexing (DWDM)**

Dense Wave Division Multiplexers (DWDM) are used to multiplex optical signals at various wavelengths onto a single fiber strand for transport across an optical network at speeds from OC-48 to OC-192. Each wavelength can run at speeds of up to 10 Gbps. Current optical systems can multiplex as many as 100 wavelengths or channels per fiber strand which is almost 1 Terabit (1000 Gbps) aggregate speed. Current efforts are focused on developing multi-terabit transport on 1 fiber strand. This technology is somewhat of a demarcation between the fastest enterprise core networks and the long haul ISP core networks which aggregate hundreds of enterprise customers. The enterprise customer can connect with DWDM networks using ATM switches and IP routers with OC-48 interfaces. Public and private SONET network providers have rings that

connect using equipment with interfaces running at OC-48 speeds as well. The Cisco 12016 Gigabit switch router is available with OC-48 interfaces. Companies today are utilizing 400 OC-48 router interfaces at the 12016 to build a Terabit WAN core.

### **Data Link Switching (DLSW+)**

Data Link Switching is a Layer 2 protocol used for encapsulating SNA frames across an IP WAN. It is an IP encapsulation method that integrates SNA workstations and servers with the IP enterprise network. Encapsulation of SNA is required since there is no Layer 3 addressing defined with its protocol stack. Routers that are configured with DLSW+ will establish peer relationships with local and remote DLSW+ routers. Each SNA Frame is encapsulated in an IP packet before it is sent across the WAN to a peer router configured with DLSW+. Each local router will terminate LLC2 data link layer frames from each workstation and send local acknowledgments to each local workstation as packets are sent and received. That eliminates LLC2 timeout issues that can occur between workstation and server when acknowledgments must travel across a congested WAN circuit.

SNA is connection-oriented and must receive data link acknowledgments every few seconds or the session will timeout. Bridge protocols such as Source Route Bridging (SRB) limit the number of bridges and rings that an SNA packet can span. There is no issue with the number of Rings utilized with DLSW+ since the RIF field is terminated at the router. DLSW+ integrates many different data link technologies such as Ethernet, Token Ring, SDLC and Frame Relay. There is a translation as well between different frame types such as Ethernet and Token Ring at each router for those data link technologies. Promiscuous mode is configured at DLSW+ routers which allows for many connections from remote peer routers. An example would be 7500 Data Center routers that have peer connections from many distribution offices.

## **WebSphere**

### **Definition**

[WebSphere](#) is a product line from IBM featuring web-based applications. The term WebSphere is usually used in reference to the actual Web application server (WAS). The WAS is a Java-based server that delivers content to end-users and allows Java-based applications to interact with the remote users usually via the HTTP protocol.

### **Business applications**

For businesses, WebSphere offers a platform to grow Java applications to a highly robust, high performance system. WebSphere works on all IBM platforms, mainframes, AIX, Linux, and Windows. It provides a single development platform for the business and provides tools from development to production application management.

### **Controversies**

The WAS product from IBM has many competitors; most notable is the [Tomcat server](#) from the Apache group. Many users have gone over the fence, either to Tomcat or to [WebSphere](#). The outcomes are mixed, and it might boil down to personal preference on which system the administrator or developer likes to use their applications. WebSphere is a family of products beyond the WAS, so in Java environments that need an entire application development environment from start to finish, and where extensive support is needed, WebSphere is a good option.

## **Technical details**

According to the [IBM WebSphere website](#), WebSphere Application Server V7 offers three attributes that make capable the development of robust, agile business applications: Simplified Development, Intelligent Management, and High Performance.

## **Web Services**

### **Definition**

There are two ways the term Web services can be used. One refers to standards-based software accessible over the Web. That is the definition used by Amazon and others who offer Web services online to businesses for a fee. These Web services often rely on HTTP and are referred to as RESTful Web services. RESTful Web services do not use XML or SOAP.

But Web services can also be used in a slightly different way, and it is this definition that is most common when you talk about using Web services in enterprises to support, for instance, a service-oriented architecture. In this case, the [W3C's definition](#) might be more helpful: “A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.”

### **Business applications**

There are a number of business uses for Web services. One of the most obvious business uses is the ability to subscribe to Web services online or even offer your own Web services to clients or business partners via the Internet. Web services can be combined to provide new software and services, as well.

Web services can also be used for application integration, linking applications, [according to WiseGeek.com](#). Since Web services can use HTTP and so work through the firewall, which means you don't have to deal with special security protocols. It should be noted, however, that Web services can also use File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP) and Extensible Messaging and Presence Protocol (XMPP) for exchanging data.

Web services can also form the foundation for service-oriented architecture or a Web-oriented architecture.

## **Deployment Concerns**

One issue to consider is whether you'll use a SOAP-based approach or a RESTful approach to Web services. Much has been written about the pros and cons of each. Here are a few notes on the pros and cons of each.

SOAP – SOAP-based Web services are supported by software vendors in SOAP WS toolkits, which make it easy for enterprises to deploy on SOAP. RESTful critics claim that changes to the SOAP stack could cause problems with the service. Critics also say the use of XML as a messaging tool could create unnecessary overhead and slow down the service.

REST – RESTful Web services are supposed to be easier and leaner than SOAP-based Web services. [Amazon.com](http://Amazon.com) claims 80 to 85 percent of its Web services clients use REST. The main problem with REST is it's not supported by major vendors or their software development tools. Others point out REST is so easy to build, you don't need a toolkit.

Dion Hinchcliffe [wrote an overview of the REST](#) versus SOAP debate in 2005 that's still useful today.

## **Windows 7**

### **Definition**

Previously [identified](#) as “Blackcomb” and “Vienna,” [Windows 7](#) is reported to be the next version of the Windows OS. It will succeed Windows Vista, will be available in both client and server versions, and will be released on October 22, 2009.

### **Business applications**

Windows 7 client and server, will offer enhanced remote [management](#) for the enterprise, and offer a better experience for laptop users. This will be a positive purchase-point for businesses when the software ships. Since it is being built with the compatibility of the Windows operating systems, millions of applications will be available for the system, thereby reducing most conversion costs for the enterprise.

### **Controversies**

Microsoft has reported that the new OS will contain [performance improvements](#) over the current Windows Vista. This may be a tipping point for some businesses to move to the new OS. Vista has had its problems with [adoption](#) by the mainstream and businesses. The much-awaited new version of the Windows OS really needs to live up to the hype to succeed.

### **Technical details**

Windows 7 will be available in 32- and 64-bit versions. The dreaded [UAC](#) that came with Windows Vista has been enhanced to allow the user to control how often they are notified of changes to the system. There are also some personalization changes that allow each user to define their desktop, as well as enhancements to the wireless networking controls. As far as technical changes, it should be very similar to Vista, but with some aesthetic changes to clear up the issues that have plagued Vista.

## Windows Server Platforms

### Definition

Microsoft offers various versions of its Windows operating systems especially for server based applications. The most recent version is [Windows Server 2008](#), which was launched in February of 2008. Microsoft uses the same framework for its workstations and servers, but for the server platform, alterations are made to the configuration to allow for multi-user and application speed and reliability.

### Business applications

Many enterprises use a [version of Windows Server](#) on their servers to help centralize applications deployment for end users. The platform provides file and printer sharing, authentication and authorization, web and database application farms, and custom written applications. There are also Web editions to help build and host web applications.

### Concerns

The major concern with using the Windows Server as your application and database platform is reliability. There have been several cases of [virus and malware](#) issues with Windows Server platforms. To deal with these issues, Microsoft releases patches nearly [every Tuesday](#). Installing patches and updates often causes an increased amount of server downtime and administrator time to keep the systems running securely.

### Technical details

There are 32- and 64-bit versions of Windows Server 2008. This version is tuned for application speed and reliability (as compared to the Vista workstation version). There are a number of security modifications to protect the multi-user system and also [additional services](#) that are not provided on the desktop version, such as IIS (Web server), DNS, DHCP servers, and [Active Directory](#) to allow for simplified management of users and computers. The server platform offers the same interface as the desktop version, which provides a familiar environment in which the administrators can operate. Windows Server platform is available only for Intel and AMD x86 based CPUs, but it supports a vast array of server-class hardware from Dell, IBM, and HP such as RAID, SAN, and networking peripherals.



## Windows Vista

### Definition

Windows Vista was released in January 2007 and its primary objective was to improve security in the Windows OS. It has been received with mixed reviews—its new features and improved security have been cheered, while it has been [criticized](#) for a multitude of other reasons.

### Business applications

Vista provides numerous deployment and maintenance technologies including WIM (Windows Imaging Format), Windows Deployment Services, 700 new Group Policy settings, and a multilingual user interface. The Windows Vista OS also offers a [Business upgrade](#) that provides a variety of tools and features for small businesses.

### Controversies

Early after its release, Vista was clobbered with numerous criticisms and complaints. Issues such as large system resource requirements, restrictive licensing agreements, and problems with the User Account Control (UAC) have dogged the OS since its release and [continue to make users](#)—and businesses—wonder whether it's worth the price of an upgrade.

### Technical details

There are six editions of Windows Vista; Windows Vista Starter, Windows Vista Home Basic, Windows Vista Home Premium, Windows Vista Business, Windows Vista Enterprise, and Windows Vista Ultimate. [Vista capable computers are required to have](#) at least an 800 MHz processor, 512 MB of memory, DirectX 9.0 capable graphics card, 32 MB graphics memory, and 20 GB HDD capacity. However, to fully utilize some of the special options and high-end graphics features, it is recommended that your system have 1 GHz processor, 1 GB memory, DirectX 9.0 and WDDM 1.0 driver support, 512 MB graphics memory, and 40 GB HDD capacity.

## Windows XP

### Definition

Released in late 2001, [Windows XP](#) is the first OS meant for consumer use that was built on the NT kernel. It was released with several versions, including Windows XP Home, XP Professional, and XP PC Tablet edition. It succeeded Windows 2000 Professional and Windows Me.

### Business applications

[Windows XP Professional](#) was marketed to power users and enterprises. It provided support for two physical processors and Windows Server domains. It was notably more stable than previous Windows 9.x versions and was more user friendly with its task-bar based interface.

## **Concerns**

The most recent issue with Windows XP has been the worry over when Microsoft will end its support of XP. [According to Microsoft](#), though, support for this favored OS will now continue through 2014.

## **Technical details**

[Windows XP Service Pack 3](#) is the most recent update to the OS. It contains security fixes, updates Windows Media Center, and provides several new features including Windows Imaging Component, the Network Access Protection client, and default detection of black hole routers.

## **Wireless Network Components**

### **Client Software and Adapter**

Any client computer, laptop or wireless device with a compatible wireless client adapter allows connectivity with an access point. The client adapter is a radio transmitter with firmware that supports any of 802.11a/b/g signaling. That is needed before the device can associate and authenticate with the access point. Some access points have a no client mode that doesn't allow any association from clients extending network distance. Client wireless software included with the adapter must be implemented with specific Windows platforms. The client adapter will be integrated with the laptop, PCMCIA slot or desktop PCI bus slot. They will support specific wireless standards, antenna characteristics, WiFi certification, WDS, network range and security. The wireless manufacturer software must be implemented for all available features. The following is a list of some client adapter configured settings.

### **Access Point**

As the name suggests an access point allows connectivity between the wireless client or wireless device and the wired network. The access point takes wireless data packets from a client and translates them to standard Ethernet data frames before transmitting across the wired network. Standard category 5 twisted pair cabling will connect the access point Ethernet port with a catalyst switch Ethernet port. The maximum distance between access point and network switch is 100 meters standard with Ethernet design.

### **WLAN Controllers**

Wireless designs with hundreds of root access points on an enterprise network will sometimes deploy wireless LAN controllers. The design specifies lightweight access points connecting to a network switch. The 4404 WLAN controller device acts as a hub connecting 4 network switches supporting 100 access points. Cisco wireless control system (WCS) wireless network

management software is sometimes deployed with WLAN controller design for planning, configuring and optimizing the network.

## **Power Injector**

Cisco access points have a variety of power options such as AC adapters, power over Ethernet and power injectors. The placement of access points is such that in some situations an AC power outlet isn't available. Should your Ethernet switch not support power over Ethernet, an option such as power injectors extends the distance from an AC outlet. Distances of 1.24 miles are available with a fiber optic media converter.

## **Power over Ethernet**

Cisco access points can be deployed with power over Ethernet (PoE) should the network switch modules support that feature. The distance of 300 feet is the same with Cisco prestandard and 802.3af. The Cisco prestandard use Cat 5 cabling pins 1, 2, 3, 6 for powering devices while 802.3af uses 1, 2, 3, 6 with 10/100/1000BaseT signaling and 4, 5, 7, 8 with 10/100BaseT. Select a network switch module with the power over Ethernet standard your access point has implemented and has a power wattage rating per port for your specific devices. The network switch power supply should be upgraded to support additional power draw from multiple devices. Deploying power over Ethernet will decrease implementation costs with deployment of IPT, wireless and Gigabit. See network switch documents at Cisco web site for information on what network switching modules support PoE and wattage ratings. 802.3af defines powered device class 2 at 3.84W - 6.49W and class 3 at 6.49W - 12.95W.

## **Power Patch Panel**

Cisco inline power patch panels can be deployed where Ethernet switches don't support power over Ethernet and power injectors aren't an option. The patch panel does no switching. It powers the devices through a Cat 5 cable that is a maximum 300 feet at a specific rated wattage per port. The patch panel connects the access point to the wired switch with a patch cable.

## **Wireless Network Security**

This article addresses the terms and basics of securing a Wireless LAN.

### **Network Authentication Process**

The process of a client associating and authenticating to an access point is standard. Should shared key authentication be selected at the client, there are additional packets sent confirming the keys authenticity.

The following describes EAP network authentication.

1. Client sends probe to all access points

2. Access point sends information frame with data rate etc
3. Client selects nearest matching access point
4. Client scans access point in order of 802.11a, 802.11b then 802.11g
5. Data rate is selected
6. Client associates to access point with SSID
7. With EAP network authentication the client authenticates with RADIUS server

### **Open Authentication**

This type of security assigns a string to an access point or several access points defining a logical segmented wireless network known as a service set identifier (SSID). The client can't associate with an access point unless it is configured with that SSID. Associating with the network is as easy as determining the SSID from any client on the network. The access point can be configured to not broadcast the SSID improving security somewhat. Most companies will implement static or dynamic keys to supplement security of SSID.

### **Static WEP keys**

Configuring your client adapter with a static wired equivalency private (WEP) key improves the security of your wireless transmissions. The access point is configured with the same 40 bit or 128 bit WEP key and during association those encrypted keys are compared. The issue is hackers can intercept wireless packets and decode your WEP key.

### **Dynamic WEP keys (WPA)**

The deployment of dynamic encrypted WEP keys per session strengthens security with a hash algorithm that generates new key pairs at specific intervals making spoofing much more difficult. The protocol standard includes 802.1x authentication methods with TKIP and MIC encryption. Authentication between the wireless client and authentication RADIUS server allows for dynamic administration of security. It should be mentioned that each authentication type will specify Windows platform support. An example is PEAP which requires Windows XP with service pack 2, Windows 2000 with SP4 or Windows 2003 at each client.

The 802.1x standard is an authentication standard with per user and per session encryption with these supported EAP types: EAP-TLS, LEAP, PEAP, EAP-FAST, EAP-TTLS and EAP-SIM. User network authentication credentials have nothing to do with the client computer configuration. Any loss of computer equipment doesn't affect security. The encryption process is handled with TKIP an enhanced encryption standard improving WEP encryption with per packet key hashing (PPK), message integrity checking (MIC) and broadcast key rotation. The protocol uses 128 bit keys for encrypting data and 64 bit keys for authentication. The transmitter adds some bytes or MIC to a packet before encrypting it and the receiver decrypts and verifies the

MIC. Broadcast key rotation will rotate unicast and broadcast keys at specific intervals. Fast reconnect is a WPA feature that is available allowing employees to roam without having to re-authenticate with the RADIUS server should they change floors or rooms. The client username and password is cached with the RADIUS server for a specified period.

### **EAP-FAST**

- Implements symmetric key algorithm to build secure tunnel
- Client and RADIUS server side mutual authentication
- Client sends username and password credential in secure tunnel

### **EAP-TLS**

- SSL v3 builds an encrypted tunnel
- Client side and RADIUS server side assigned PKI certificates with mutual authentication
- Dynamic per client per session keys used to encrypt data

### **Protected EAP (PEAP)**

- Implemented at Windows clients with any EAP authentication method
- Server side RADIUS server authentication with root CA digital certificate
- Client side authentication with RADIUS server from Microsoft MS-CHAP v2 client with username and password encrypted credentials

### **Wireless Client EAP Network Authentication Process**

1. Client associates with access point
2. Access point allows 802.1x traffic
3. Client authenticates RADIUS server certificate
4. RADIUS server sends username with password encrypted request to client
5. Client sends username with password encrypted to RADIUS server
6. RADIUS server and client derive WEP key. RADIUS server sends WEP key to access point
7. Access point encrypts 128 bit broadcast key with that dynamic session key. Sends to client.

8. Client and access point use session key to encrypt/decrypt packets

## **WPA-PSK**

WPA pre-shared keys use some features of static WEP keys and dynamic key protocols. Each client and access point is configured with a specific static passcode. The passcode generates keys that TKIP uses to encrypt data per session. The passcode should be at least 27 characters to defend against dictionary attacks.

## **WPA2**

The WPA2 standard implements the WPA authentication methods with Advanced Encryption Standard (AES). This encryption method is deployed with government implementations etc. where the most stringent security must be implemented.

## **Application Layer Passcode**

SSG uses a passcode at the application layer. Client can't authenticate unless they know the passcode. SSG is implemented in public places such as hotels where the client pays for the password allowing access to the network.

## **VLAN Assignments**

As noted companies will deploy access points with SSID assignments that define logical wireless networks. The access point SSID will then be mapped to a VLAN on the wired network that segments traffic from specific groups as they would with the conventional wired network. Wireless deployments with multiple VLANs will then configure 802.1q or ISL Trunking between access point and Ethernet switch.

## **Miscellaneous Settings**

- Turn Microsoft File Sharing OFF
- Implement Antivirus Software and Firewall
- Install your company VPN client
- Turn OFF Auto Connect to any wireless network
- Never use AdHoc Mode - this allows unknown laptops to connect
- Avoid signal overrun with a good site survey • Use minimal transmit power setting

## **Anti-Theft Option**

Some access points have an anti-theft option available using padlock and cabling to secure equipment while deployed in public places. This is a key feature with public implementations where access points can be stolen or there is some reason why they must be mounted below the ceiling.

## **Security Attacks**

- Wireless packet sniffers will capture, decode and analyze packets sent between the client computer and access points. The purpose is to decode security information.
- Dictionary attacks attempt to determine the decryption key configured on the wireless network using a list or dictionary with thousands of typical passcode phrases. The hacker captures information from the authentication process and scans each dictionary word against the password until a match is found.
- The specific mode assigned each wireless client affects security. Ad Hoc mode is the least secure option with no access point authentication. Each computer on the network can send information to an Ad Hoc neighbor computer. Select infrastructure mode where available.
- IP spoofing is a common network attack involving faking or replacing the source IP address of each packet. The network device thinks its communicating with an approved computer.
- SNMP is sometimes a source of compromised security. Implement SNMP v3 with complex.

## **Wireless Network Standards**

The following describes the current defined wireless protocol standards.

### **802.11a**

This standard was approved in 1999 with the IEEE committee. It specifies a maximum data rate of 54 Mbps using 5.15 GHz - 5.35 GHz and 5.725 GHz - 5.825 GHz unlicensed bands in the United States. The advantage of 802.11a is higher throughput however the cell coverage is smaller and additional access points will be needed. There is much less interference from devices such as cell phones, microwaves and commercial devices using the 2.4 GHz band. There are 23 non-overlapping channels with the current 802.11h specification. Some Cisco devices support both 2.4 GHz and 5 GHz transmitters on the same access point. The modulation scheme used with 802.11a is OFDM which is effective, allowing higher data rates and minimizes effects of interference. An advantage of 802.11a is the continued deployment around the world however each country specifies number of channels and frequencies with the 5 GHz band. It is a good practice to separate neighbor channels with non-neighbor assignments.

### **802.11b**

This standard was approved in 1999 with the IEEE committee. It specifies a maximum data rate of 11 Mbps using the 2.412 GHz - 2.484 GHz unlicensed band in the United States. That band experiences a lot of interference from commercial devices using that frequency. The standard in the United States specifies 11 channels with a bandwidth of around 80 MHz at 5 MHz per channel. The United States allocates 3 non-overlapping channels of 1, 6 and 11 with center frequency separation of 25 MHz per channel. The modulation scheme used with 802.11b is Direct Sequence Spread Spectrum (DSSS) with CCK which has characteristics that minimize affects associated with interference. 802.11b transmit speeds include 1, 2, 5.5 and 11 Mbps.

### **802.11g**

This standard was approved in 2003 with the IEEE committee. It specifies a maximum data rate of 54 Mbps using the same 2.4 GHz band as 802.11b. The 802.11g standard is most popular around the United States with high throughput, increased coverage and less cost. The same interference occurs however with the 2.4 GHz band. The 802.11g is compatible with 802.11b standard and assigns the same 11 channels with 1, 6 and 11 as non-overlapping. The modulation scheme used with 802.11g is OFDM with higher data rates specified. 802.11g specification has transmit speeds including 6, 9, 12, 18, 24, 36 and 48 Mbps.

### **802.16**

This is a wireless standard focused on MAN implementations allowing home and office seamless wireless access from devices anywhere across a metropolitan city with line of sight distances of around 27 miles and speeds of 120 Mbps. The point to multipoint specification operates in the 10 - 66 GHz range. There is an 802.16a specification with mesh topologies and non line of sight that describes frequencies from the licensed and unlicensed 2 GHz and 11 GHz band at a speed of 70 Mbps. The key issue with any MAN implementation and all fixed wireless has to do with interference and frequency your equipment is assigned. The unlicensed frequencies will of course be vulnerable to interference from similar devices across the city.

### **802.11n**

This new standard specifies faster rates of 600 Mbps between access points and 1000 Mbps from access point to network switch increasing throughput from the current 100 Mbps.

### **Wi-Fi Alliance Forum**

Tests and certifies manufacturer wireless products for conformity with specific wireless standards. Devices that have been certified interoperable can be deployed in mixed multi vendor environments.

### **XML**

### **Definition**



XML is an acronym for eXtensible Markup Language. It is an open standards markup languages created by the World Wide Web Consortium. It's called a metalanguage, which simply means it is a language that describes other languages.

[XML was originally designed](#) for large-scale electronic publishing and derived from the Standard Generalized Markup Language (SGML), according to the W3C.

XML is more a set of standards than a language. That's why it's possible to create your own XML schema, or markup vocabulary.

## **Business applications**

The financial world uses an XML-based language, XBRL (eXtensible Business Reporting Language), to [help transfer data and report financial results](#), according to Wikipedia. Other use cases mentioned by Wikipedia are for large documentation, including maintenance books for manufacturing, and maps.

The [XML FAQ](#) lists the following other uses for XML:

1. Information identification
2. Information storage
3. Information structure
4. Messaging and data transfer
5. Web services

Because of its support for tagging and its messaging and data transfer capabilities, XML also acts as an underlying technology for many business solutions, including EII and porting information to [wireless devices](#).

## **Deployment Concerns**

There are some who believe XML is being overused and adds an unnecessary “layer of overhead” to data integration. Cliff Longman of Kalido, which sells business intelligence and master data management solutions, offered cautionary advice about over-reliance on XML in this [Q&A](#) with IT Business Edge.

## **Technical details**

Other programs can use XML to extract data from information because XML tags conform to a model. For a simple example of how XML applies tags to data, check out [this entry on Wise Geek](#).

You can also find resources on the XML specifications at the [W3C](#)



*Copyright © 2003-2011 NarrowCast Group, LLC. All rights reserved.*  
<http://www.itbusinessedge.com>