Cisco 2008 Annual Security Report

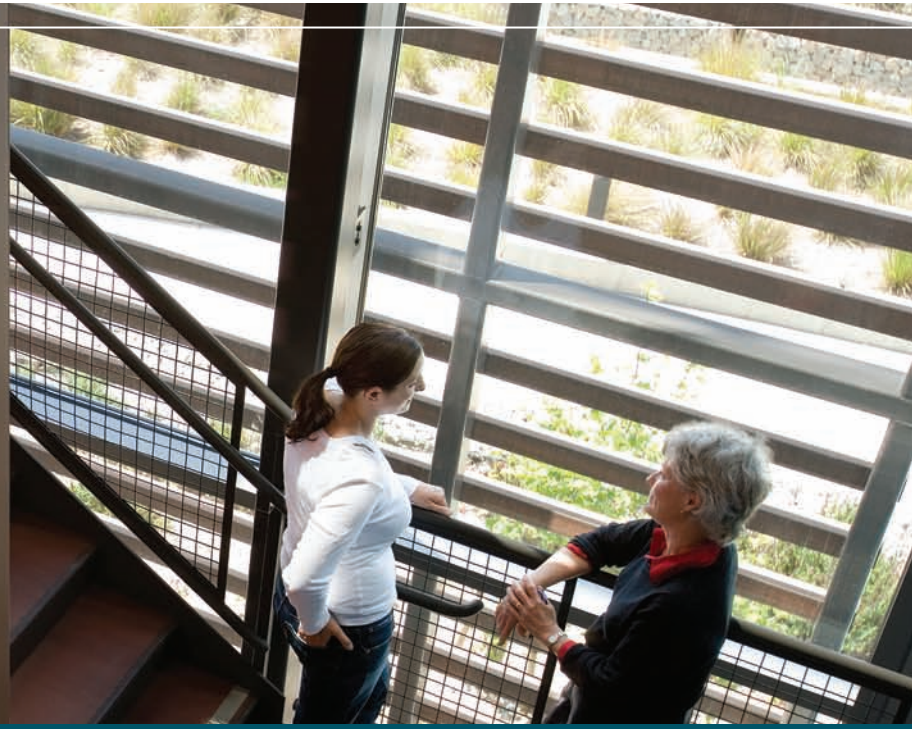
Highlighting global security threats and trends

CISCO

Contents

The Cisco® Annual Security Report provides an overview of the combined security intelligence of the entire Cisco organization. The report encompasses threat information and trends collected between January and October 2008, and provides a snapshot of the state of security for that period. The report also provides recommendations from Cisco security experts and predictions of how identified trends will continue to unfold in 2009.

Introduction



There was an enormous amount of activity related to data and online security during the past year. Although no single, overwhelming attack—such as the spread of Melissa, Slammer, or Storm malware in previous years—turned into the signature security event of 2008, the need for increased security protection and continued vigilance remains.

Compared to previous years, online criminals are becoming even more sophisticated and effective, employing a greater number of relatively smaller, more targeted campaigns to gain access to sensitive data. Human nature—in the forms of insider threats, susceptibility to social engineering, and carelessness that leads to inadvertent data loss—continues to be a major factor in countless security incidents. And the increasing use at many organizations of technologies designed to increase collaboration and productivity (such as mobile devices, virtualization, cloud computing, and other Web-based tools and Web 2.0 applications) is stretching the edges of corporate networks, potentially increasing security risks.

Many different entry points or "threat vectors" are used to compromise the security of individuals and organizations. For example, threats can be aimed at mobile devices and insecure hardware; at weaknesses in operating systems, office productivity applications, and encryption tools; and at numerous other vectors.

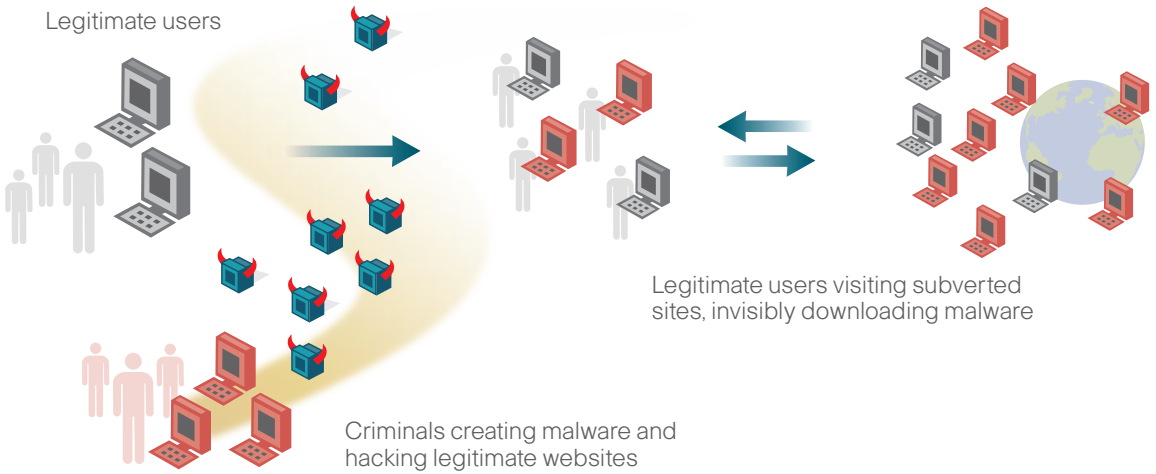
Online Threats

In terms of quantity and pervasiveness, the most significant security threats in 2008 involved an online component. These online threats continue to grow in scope and number, and should remain a top concern for security professionals.

Many of these online threats combine the following closely related elements:

- The World Wide Web
- Malware
- Botnets
- Spam

Online Criminal Ecosystem



The Web

In the online threat arena, the entire Web ecosystem comes into play. Online criminals continue to create malicious websites—carefully designing them to look alluring and legitimate—to obtain sensitive personal information or distribute malware to site visitors. They hack legitimate websites from trusted organizations, such as news media or large retailers, to cause those sites to invisibly distribute malware to visitors; they also create or subvert existing Web applications and plug-ins for the same purpose. In addition, in the core underlying infrastructure of the Internet, weaknesses have been exposed that could let online criminals divert thousands of unsuspecting Internet users at once to malicious websites.

Malware

Although far from the only method, the Web has become the primary means of infecting computers with malicious software. Most modern "malware" is designed to help someone gain control over a computer, communications device, or network. Some malware directly influences or changes an infected computer's activities—for example, causing it to connect to the Internet or install additional malware without the user's knowledge. Other malware works to find sensitive information, such as user passwords and credit card numbers, on a computer or network, and sends that information "home" to online criminals. In addition, an increasing amount of malware is being developed and sold.

Botnets

The core mission for much of today's malware is to infiltrate a computer and make it part of a botnet. Botnets consist of thousands of malware-compromised computers (botnet nodes or "zombies"), and they have become the cornerstone of large-scale online criminal activity. The people controlling botnets can rent out the processing power and bandwidth of these subverted computers to others, or use it themselves to send out massive amounts of spam, attack websites, or engage in other nefarious behavior.

Spam by Originating Country for 2008

Originating Country	Percentage of Global Spam
USA	17.2%
Turkey	9.2%
Russia	8.0%
Canada	4.7%
Brazil	4.1%
India	3.5%
Poland	3.4%
Korea	3.3%
Germany	2.9%
United Kingdom	2.9%
Thailand	2.8%
Spain	2.8%
Italy	2.4%
Argentina	2.1%
Columbia	2.1%
France	2.0%
Other	26.7%

Spam

Spam, or unsolicited email, is one of the most pervasive Internet threats, affecting nearly every Internet user and organization in the world. Different types of spam include:

- Email messages promoting items such as pharmaceuticals, printer cartridges or corporate equity instruments for sale.
- Email messages with an attached file that contains malware.
- "Phishing" emails that lure recipients into providing personal information via a return email or by filling out forms on a website.
- Email messages that include URLs and attempt to convince recipients to visit seemingly trustworthy websites that actually distribute malware.

Many spammers still blast out "mass-mailing" spam to millions of untargeted recipients per campaign; many anti-spam products work on filtering out these types of messages. But for more sophisticated "phishing" spam—which is designed to elicit personal or financial information—smaller, more targeted campaigns are becoming the norm.

Spammers continue to improve the design and effectiveness of their messages. They're using highly topical subject lines, far more legitimate-looking and professional-sounding content, and other techniques that make certain types of spam hard to resist for normally wary recipients—and easier to slip by anti-spam solutions.

To actually send out their spam messages, online criminals rarely use computers in their physical possession, instead renting or building botnets to do the mailing for them. This completes an elegant cycle, in which:

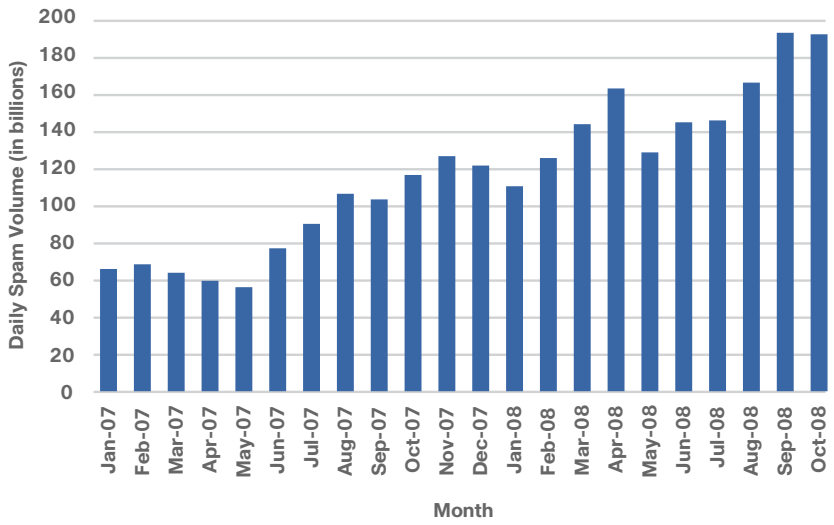
- Botnet nodes send out spam.
- Spam recipients get an email message that lures them to a malicious website.
- The website downloads malware onto the site visitor's computer to gain control over it.
- The compromised computer becomes part of a botnet, and starts sending out spam.

Data Loss

Data loss often occurs through the loss or theft of equipment such as laptops or removable storage media, or when a computer or network is infiltrated to steal sensitive data or intellectual property. Fewer organizations and individuals may be affected by data loss incidents than by online threats, but the impact of these events can be devastating.

For organizations that experience data loss, reputations and trust can be damaged or destroyed, while financial consequences such as stock-price drops, lawsuits, and compensatory damages to affected individuals can run into millions or even billions of dollars. For individuals, the consequences of a data loss incident that compromises highly personal information, such as Social Security numbers or financial details, can negatively affect their lives and finances for years.

Average Daily Spam Volume



Daily spam volumes have nearly doubled in 2008 relative to 2007.

Legislation and industry initiatives focused on making data on networks more secure and informing parties affected of data breaches are increasing. Many organizations are working to better enforce their existing acceptable use policies around sensitive data. Yet compliance with such policies and initiatives is not a guarantee of safety, as the growth and evolution of data loss threat factors are likely to outpace the initiatives or legislation addressing them.

Insider Threats

Sometimes, the people responsible for data loss and other security incidents are insiders, including current or former employees who want to cause trouble or are simply looking for personal gain. This type of threat can be especially grave, as insiders know the weaknesses in an organization's security and how best to exploit them to steal data or money, or even hold assets for ransom. In today's uncertain economy, in which more employees may lose their jobs or become dissatisfied with their work situation, and in which less budget may be available to address security concerns, insider threats —and the likelihood of their success—are of increasing concern.

Vulnerabilities

In addition to taking advantage of aspects of human nature (such as curiosity, trust, and carelessness), criminals are getting access to computers and networks by exploiting weaknesses in technologies, software, and systems.

In 2008, vulnerabilities in the entire Web ecosystem—browsers; helper objects, media players, and plug-ins running in those browsers; Web server and application software; and core parts of the underlying infrastructure of the Web—were exploited to gain control of computers, networks, and data.

Top Security Concerns of 2008

Threats and criminals are becoming faster, smarter, and more covert.

- Specialization and innovation in the online crime economy continues.
- Attacks are increasingly targeted to help maximize their effectiveness.
- Many types of reputation hijacking (attacks that exploit users' trust in someone's reputation) are gaining in prevalence and popularity.
- Blended threats that combine email and websites and use social engineering techniques are now more common than ever.

Criminals are exploiting vulnerabilities along the entire Web ecosystem to gain control of computers and networks.

- Botnet infestations remain common and dangerous.
- Known vulnerabilities are going unpatched and existing security policies are being ignored.
- Widespread use of Web-based collaborative technologies in the workplace brings added risks as well as greater productivity.

"Invisible threats" (such as hard-to-detect infections of legitimate websites) are making common sense and many traditional security solutions ineffective.

Loss of data and intellectual property are continual challenges.

- Data loss is often caused by exploiting vulnerabilities in technology and human nature.
- A company's reputation, trust and finances can be affected.
- Risk vectors include online threats, mobile devices, and insiders.

Other vulnerabilities can be exploited as well, including (among others) weaknesses in office productivity applications, operating systems, mobile device technologies, networking equipment, virtualization tools, and encryption technologies. However, vendors of affected products are now often disclosing vulnerabilities—and releasing patches at the same time—to mitigate the effects of the vulnerability, making staying up-to-date on patches more important than ever.

Online Security Risks and Trends

Online security threats continued their growth in 2008. Online criminals combined spam, phishing, botnets, malware, and malicious or compromised websites to create highly effective blended threats that use multiple online vectors to defraud and compromise the security of Internet users.

The Web itself is a primary mechanism for distributing malware that lets someone gain control over computers and networks. Many of these computers are then turned into nodes in a botnet, where they engage in a variety of activities, usually without the computer user ever being aware that this is happening.

These activities can include sending massive volumes of spam—designed to either lure more victims to websites where they'll download malware, or to obtain personal information—hosting malicious websites or infecting legitimate websites, and helping to overwhelm websites or computer networks with distributed denial of service (DDoS) attacks.

Web Trends

Fifteen years ago, barely anyone knew what the World Wide Web was. Today, Google is one of the top trusted brands in the world, and people extensively use the Web for everyday activities such as communication, research, shopping, and financial matters.

Unlike its earliest predecessors, the modern Web browser provides an amazing, highly interactive experience. Flash animation ads play within a webpage; audio streams on the websites of bands or online radio stations let site visitors listen to music; videos play automatically; social networking sites and widgets integrate contact information, photos, or data from a person's blog with their social networking page; and Adobe PDF documents render seamlessly within the browser.

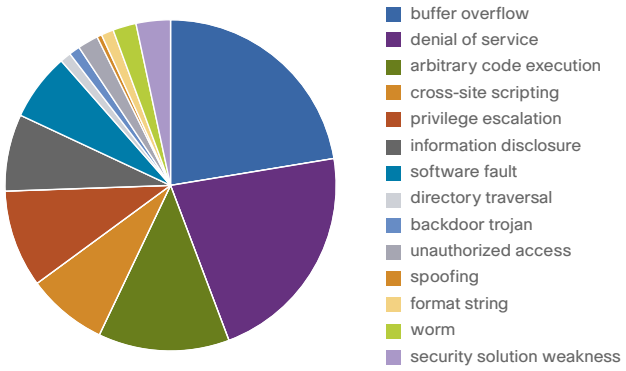
This is all possible because the Web browser uses plug-ins, media players, browser helper objects, and tools like ActiveX controls and JavaScript commands to activate different types of objects on a webpage. Underlying Web applications such as content management systems show the right content at the right time, while forums and wikis let site visitors quickly post to and modify webpages.

As the possibilities and popularity of the Web have grown, so has its use as a threat vector.

Originally, malicious software was distributed via floppy drives and macros in infected office documents, then via network worms such as Slammer, followed by an enormous rise in distribution via email. Today, a vast quantity of malware is downloaded from websites. Criminals exploit vulnerabilities throughout the entire Web ecosystem to gain control of computers and networks. (For more specific examples and information, see the *Vulnerabilities* section later in this report.)

These malware infections often happen without any user intervention or awareness in what is known as a "drive-by download." Someone visits a malicious or infected website hosting exploits that look for weaknesses in the site visitor's browser or computer system. If the exploits detect a usable weakness, they start trying to download malware to the computer. This can all happen quietly in the background, without the site visitor ever clicking on a link in the infected page or finding out what's going on.

Vulnerability and Threat Categories for 2008



In 2008, vulnerability and threat activity was dominated by buffer overflows and denials of service, with arbitrary code execution being the next most prominent category.

More and more of these malicious websites involve "in-depth" attacks, where several different types of exploits that work on different weaknesses (in different browsers, plug-ins, and operating systems) are hosted on the same website. This increases the chance that each website visitor will display a weakness—and one is all that's needed—that the exploits can take advantage of to download malware to the computer.

Compromising Legitimate Websites

A method of propagating malware that reached new levels of popularity in 2008 is compromising legitimate websites to make them hubs for malware distribution. In April 2008 alone, thousands of websites were compromised and tried to infect site visitors with malware.

Causing a trusted legitimate website to host exploits or serve up malicious code is an effective way to infect computers with malware. Site visitors have no hesitation about the trustworthiness of the site; it is a legitimate site they visit for content or transactions on a regular basis. Internet security applications that depend on URL or IP address filtering also trust the website's legitimacy.

And when legitimate websites are infected, specific user groups can be targeted with great precision—for example, infecting sites aimed at students, online gamers, or business users, with the latter potentially providing channels into business networks through compromised workplace computers.

Cisco data shows that exploited websites are currently responsible for more than 87 percent of all Web-based threats. And according to security audit provider White Hat Security, more than 79 percent of the websites hosting malicious code are *legitimate* websites that have been compromised. Nine out of any 10 websites may be vulnerable to attack: Seven out of 10 are susceptible to cross-site scripting (XSS) exploits, and one in every five may be vulnerable to SQL injection attacks.

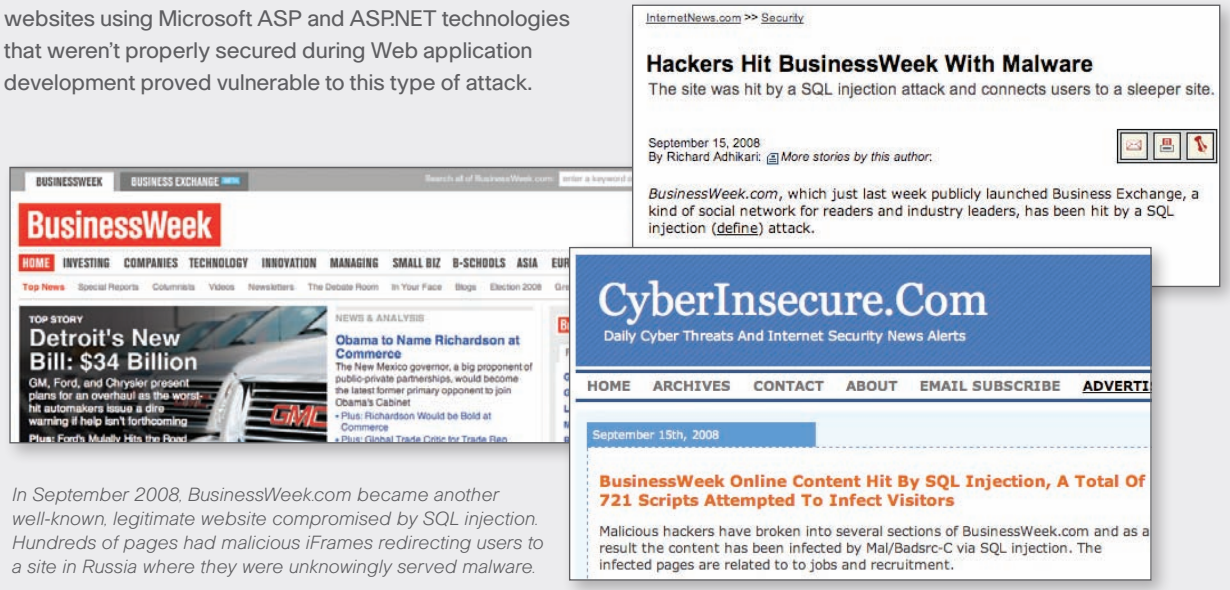
Popular Methods of Compromising Legitimate Websites

iFrame exploits. Both XSS and SQL injection exploits commonly use iFrames as a vehicle for delivering malicious code, which can install malware on a computer without the user's knowledge. An iFrame, or inline frame HTML tag, can allow the embedding of compromised Web code from another Web server into a separate HTML document. Common applications of this method include setting the size of the iFrame to zero and simply passing malicious code through the host site without the knowledge of the site visitor or the Web host.

SQL injection. Exploits a security vulnerability in the database layer of widely used Web applications and servers. Recently, hackers have used Structured Query Language (SQL) exploits to include malware or invisible links to malware-hosting sites on legitimate websites. They did this by taking advantage of website developers not properly sanitizing data transmitted in user input fields (such as forms and user logins) on webpages that use SQL. Thousands of websites using Microsoft ASP and ASP.NET technologies that weren't properly secured during Web application development proved vulnerable to this type of attack.

Cross-site scripting (XSS). A flaw within Web applications that lets ill-intentioned users of vulnerable websites or owners of malicious websites send malicious code to the browsers of unsuspecting users. These attacks are frequently executed using HTML image and frame elements (<img>, <frame>, <iframe>) and JavaScript.

Cross-site request forgery (CSRF or XSRF). An exploit in which an attacker uses the knowledge that the victim is currently engaged in a browser session on one website to forge instructions ostensibly from the victim on another site where the user is persistently or currently authenticated. For example, the attacker and victim are both online in a Web forum, and the attacker is able to steal the victim's authentication to make purchases at an e-commerce site that the attacker knows a) is frequented by the victim, and b) does not require re-authentication before finalizing purchases.



In September 2008, BusinessWeek.com became another well-known, legitimate website compromised by SQL injection. Hundreds of pages had malicious iFrames redirecting users to a site in Russia where they were unknowingly served malware.

In one notorious case in September 2008, online criminals compromised hundreds of pages on the BusinessWeek.com website with a SQL injection attack. As one of the top 1000 visited sites on the Web, BusinessWeek.com enjoys a high degree of trust from Web users. Naturally, that makes it extraordinarily attractive as a site from which to serve malware to unsuspecting visitors.

Malware Trends

A vast amount of online crime and profit is enabled by control of personal computers. The malware, or malicious software that infects these computers and turns them into botnet nodes, is the first step.

2008 was another banner year for Web-based malware. Online criminals continued employing the Web-based distribution techniques that worked so well for them in 2007, and kept refining them further for greater effectiveness and profit.

Of the malware distributed via the Web, a large portion consisted of Trojans, designed to seem innocuous, invisible, or attractive before being installed. Rootkits, which help downloaded malware stay hidden, were also prevalent. Other widely distributed malware included spyware and keyloggers, both of which send information about a compromised user's computing and Web surfing habits and personal information—including passwords—back to the malware distributors.

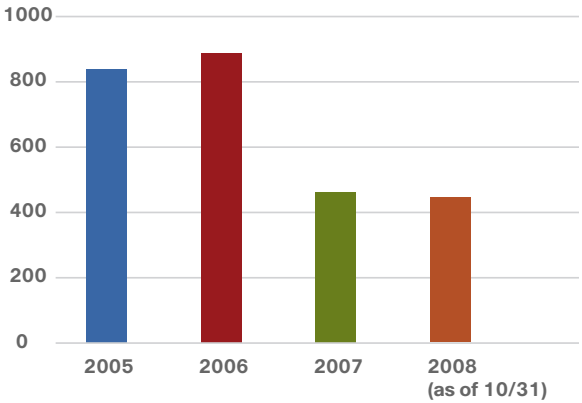
The volume of malware successfully propagated via email attachments has declined in recent years. This decline could be related to Web-based malware distribution methods proving so effective, and to the ability of anti-malware products to rapidly detect and block much of the email that contains malware. These factors may have led malware creators to spend more time on malware spread via the Web rather than via email.

Of the attachment-based malware campaigns of 2008, popular ones included messages claiming to contain delivery forms from UPS or FedEx, or messages claiming their attachment was an invoice, an e-ticket, an e-card (from Hallmark, for example), or video or pictures that were actually executable files.

Another attachment-based malware campaign shut down the IT systems of three British hospitals, when the hospitals' computer networks became infected with email-propagated Mytob malware.

To prosper, malware creators must develop tools that are tough for anti-malware solutions to detect; they are building more surreptitious malware designed to avoid detection by anti-virus and anti-malware programs. One popular technique is malware that can temporarily go dormant. Another is malware code that continually and automatically changes just enough to confuse signature-based anti-malware scanning software.

Volume of Malware Successfully Propagated via Email Attachments



The volume of malware successfully propagated via email attachments declined slightly in 2008 versus 2007. These last two years represent a 50 percent drop-off relative to the previous two years, in terms of attachment-based attacks.

Mobile Phone Malware: Growing Profit Centers

2008 saw several instances of malware designed for and spread via mobile phones.

One example is SymbOS/Kiazha.A, a "ransomware" Trojan that runs on Symbian OS devices and deletes incoming and outgoing SMS (text) messages. When it infects a mobile phone, the phone will display a message asking the user to send money (to an undisclosed location, using a mobile phone recharge card) to have the device restored to normal function.

This Trojan is installed on the phone by SymbOS.Multidropper.A, which also installs SymbOS/Beselo, a worm that propagates by sending itself as MMS (multimedia) messages every two minutes to every contact in the mobile phone's phonebook. It can also propagate via Bluetooth, and copy itself to any memory card inserted into the phone, allowing it to recover from deletion. In another tactic to enhance propagation, SymbOS.Multidropper.A installs SymbOS/ComWar.C, which spreads via Bluetooth and replicates and monitors itself to ensure it is not erased from the phone.

During the last year, malware for mobile phones was largely circulated in Asia, where the number of people who own such devices is significantly higher than those who own personal computers. This makes spreading malware via mobile phones a potentially profitable endeavor for malware creators in that region.

The "Shadow" Internet Economy

Successful online criminals are making millions or hundreds of millions of dollars from their enterprises. These profits continue to drive innovation and specialization.

Like the legitimate Internet economy they shadow, the online criminal world has become a global, thriving network of product and service providers and consumers doing business together. In the short term, this specialization and collaboration are making online criminals more nimble and effective.

Those launching attacks are often no longer the developers creating the tools. Instead, attackers can select from an array of competing and increasingly sophisticated products and solutions. A wide range of well-designed malware offerings is currently for sale or rent, including:

- Botnet management and dashboard-type tools
- Mass blog posting tools
- Sophisticated volume spamming tools
- Automated webmail account creation tools (including some that defeat the CAPTCHA feature that webmail hosts such as Yahoo!, Gmail, and MSN use to prevent bots from opening webmail accounts)
- Account generators that enable spammers and scammers to bulk-post to Craigslist
- Keylogging programs

But in the longer term, the online crime economy may also be on its way to becoming a bureaucracy. The positive side to this: One unavoidable side effect of becoming more established is a paper trail, which may make it easier for law enforcement organizations worldwide to track and apprehend more of these offenders in the future.

Asprox: Transforming an Old Trojan

One of the most effective botnets of 2008 was Asprox, an old Trojan that was turned into a very sophisticated botnet and used in thousands of SQL injection attacks on legitimate websites. First used several years ago as a password-stealing Trojan, it was later upgraded to send phishing spam. Its big transformation occurred in May 2008, when Asprox started updating itself with a SQL injection tool.

This SQL injection tool looks legitimate to users of infected computers, running as "Microsoft Security Center Extension" (msscntr32.exe). Meanwhile, in the background, it is actually using Google to scan the Web for Active Server Pages (.asp), which can be susceptible to SQL exploits.

When the SQL injection tool finds vulnerable pages, it inserts a malicious iFrame into page content. The iFrame invisibly redirects a site visitor's browser to malsites that try various methods of infecting the victim's computer with malware and adding it to the Asprox botnet. To make it harder to detect to anti-malware programs, Asprox communicates via proxy server on TCP ports 80 or 82.

Cisco data showed that at its peak, Asprox was successfully iFrame-injecting 31,000 different websites per day.

Botnet Trends

Botnets are the big "workhorses" that power many of today's online threats and criminal activities. Botnets consist of thousands of malware-compromised computers. Those who control the botnets can rent out the processing power and bandwidth available to these computers, or use it themselves.

Online criminals are using botnets for pretty much every aspect of Web-based threats, including spamming, sending DDoS attacks, infecting legitimate websites, hosting malicious websites (such as botsites), and propagating more malware.

The Storm botnet, enormously widespread in 2007, was only a harbinger of what was to come. New, even more sophisticated, robust, and scalable botnets, such as Mailer Reactor, Kraken, and an updated, powerful variant of Asprox (which had been around in a less able form for several years), have also had great success.

These botnets are designed as reusable platforms that can cycle, synchronize, and distribute dynamic attacks. Like many Web 2.0 technologies, they "promote" collaboration and depend on the network effect. They're adaptive and intelligent, and offer flexibility, redundancy, and security protocols inspired by modern peer-to-peer (P2P) networks.

The Importance of Social Engineering

Online criminals have developed an array of sophisticated social engineering techniques to entice victims to open an email or file, or to click on a link or online ad. The use and sophistication of social engineering techniques in online attacks continued to grow in 2008, and this trend is expected to continue during 2009 with even more—and even better executed—attacks occurring via email, instant messaging (IM), and mobile devices.

One successful technique is creating spam campaigns based around "hot topic" news items and current events. Sometimes, these spam emails direct victims to a malicious site that will attempt to download malware to their computers.

But more sophisticated campaigns that include extremely clever phishing websites, and where both spam and websites use social engineering techniques tied to current events, have also become common.

With those campaigns, victims are lured to legitimate-looking websites where they are asked to provide personal information during what appears to be an actual transaction. However, victims do not receive the goods or services they thought they had purchased. Or, in cases where the fraudsters do send something, counterfeit or poor-quality items are delivered—for example, fake pharmaceuticals disguised as brand-name prescription medication.

The more effective email-attachment-based malware distribution campaigns of 2008 also used clever social engineering techniques.

One type involved email claiming to be from UPS or FedEx, which asked the recipient to review an attached invoice or delivery confirmation to discover what happened to a fictitious package. When the victim opened the attachment, the malware installed itself and let the attacker gain control over the infected computer.

> "These virus-laden emails that claim they're from FedEx or UPS are really clever. It's no wonder people respond to them!"
>
> —Michael Postlethwait, Cisco Security Analyst

Another notable campaign occurred around U.S. tax-filing time. This one involved email that looked as if it had been sent by the Internal Revenue Service (IRS). It had a very official appearance, and played on the widespread fear of the IRS and worries about not opening or responding to its letters. Only the most savvy recipients realized that the IRS does not send notifications in email, but only uses paper mail sent via the U.S. Postal Service.

The continuing popularity of "scareware" can also be explained by viewing it as an example of successful social engineering techniques. Scareware pretends to be anti-malware or anti-spyware scanning software, but is actually malware that is taking advantage of computer users' fear of spyware or malware to infect them. The websites these downloads are offered from often look extremely credible and professional, and often include fake logos and endorsements from industry organizations.

New President, New Malware

Current events-oriented email messages convince recipients to open and act on the email. In a recent example, a spam campaign invited recipients to watch a video of President-elect Barack Obama's victory speech. Subject line examples included:

- Election Results Winner
- The New President's Cabinet?
- Obama Win Sets Stage for Showdown

The email directed recipients to a fake government-themed botsite. Once there, they were prompted to install an Adobe Flash Player update, which was actually data-stealing malware. Once installed, the malware stole screenshots and passwords, sending that information to a Web server located in Kiev, Ukraine.

Government-Themed Botsite

The Real America.gov Site

In this example, recipients of a message—which claimed to include a link to Barack Obama's victory speech—were actually directed to a botsite serving up data-stealing malware.

Beijing Olympics Fake Ticketing Scams

One of the most elaborate social engineering Internet scams of 2008 was related to the Beijing Olympics, with criminals making a profit of an estimated US$40 to $50 million. People in several countries, from New Zealand to the United States, were taken in by fake ticketing sites that sold illegitimate or nonexistent tickets to Olympic events. Some individuals paid thousands of dollars for particularly hard-to-come-by tickets, such as those for the opening ceremonies.

The biggest offender was Beijingticketing.com, a professional-looking website that featured the official Beijing Games logo. This fraudulent website was superior to the official ticketing site, with a better ticketing purchasing process and integration with social networking sites like Facebook to virally spread the fake site. Even MSNBC initially believed the site was credible: An MSNBC Forbes Traveler article featured a link to the site. This helped it gain a high search engine ranking, which resulted in ticket seekers who used search engines to look for tickets going to the fake site rather than legitimate sites.

Beijingticketing.com asked users to register—and provide confidential information—before they could purchase tickets. After registration, users provided credit card numbers and "bought" tickets, which they never received. Not only did the scammers net millions of dollars, but they also scooped up thousands of valid credit card numbers for later use or resale to other online criminals.

Scam Ticketing Site

Official Ticketing Site

Fraudulent Olympics ticketing websites, such as beijingticketing.com, took advantage of thousands eager to buy tickets to the 2008 Beijing Summer Olympics.

Source: www.beijingticketscam.com. Moriarty Leyendecker Erben LLP.

Spam and Phishing Trends

Cisco estimates that currently, almost 200 billion messages per day—or approximately 90 percent of all email sent worldwide—can be defined as spam. That's double the volume of the previous year, and represents 200 spam emails per day for every Internet user on the planet. Spam has undergone a significant evolution in the last year. Massive volumes of pharmaceutical and get-rich-quick spam from botnets remain a resource- and processing-intensive issue for many organizations and service providers. Still, the network protection, anti-spam, and filtering solutions in place at most enterprises have made high-volume, low-sophistication spam more of an annoyance than a security issue.

The spam that does ultimately make it into recipients' inboxes is becoming ever more dangerous and attractive, and thus likely to be opened. Newer spam campaigns typically include "blended threat" spam messages, which incorporate URLs to entice recipients to click through to malware-distributing or phishing websites.

Another type of spam that has become noticeably more common this year involves targeted phishing, also known as "spear phishing." For these attacks, sophisticated online criminals have been using smaller phishing campaigns aimed at more targeted groups of recipients—to great effect.

Earlier phishing campaigns were widespread and high-volume, and typically pretended to be from large banks with a national presence. Then, an increasing number of phishing campaigns started using the identities of regional and local banks located near the recipient (and thus involved fewer messages per campaign).

The latest types of spear-phishing campaigns include:

- Spam sent via SMS to the mobile phones of recipients in the same area code
- Email pretending to be from universities with which the intended victims are affiliated as current students, alumni, or faculty
- Email that attempts to lure the victim into entering login information about their Google Adwords account (not only is the victim's credit card or personal information stolen, but often, their Adwords traffic gets redirected to criminal-run blogs)
- "Whaling" emails, which are extremely personalized to target specific top executives

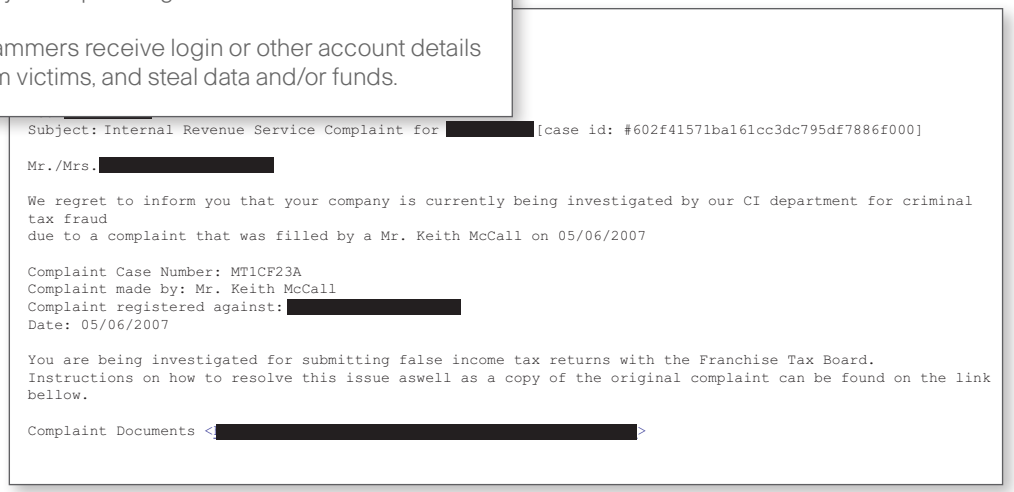
Spear-Phishing Examples

Spear-phishing messages currently represent about one percent of all phishing campaigns, but are expected to become more prevalent. This trend bears close monitoring, because the attacks are becoming more sophisticated: Criminals are investing time and resources in personalizing spam and making the messages seem credible. Why? Because the jackpots are higher when they succeed in obtaining sensitive personal data from specially targeted, attractive victims.

Typical spear-phishing attacks consist of four steps:

1. By launching malware, hacking into networks or buying lists from other nefarious online resources, scammers obtain a specialized distribution list of valid email addresses.
2. They register a domain and build a fake (but credible-looking) website to which phishing email recipients are directed.
3. They send phishing emails to their distribution list.
4. Scammers receive login or other account details from victims, and steal data and/or funds.

Spear-phishing attacks require criminals to efficiently build appropriate resources and trick victims into revealing valuable private information.



Spear-phishing emails often succeed because they mimic messages from an authoritative source, such as a financial institution, a communications company, or some other easily recognizable entity with a reputable brand.

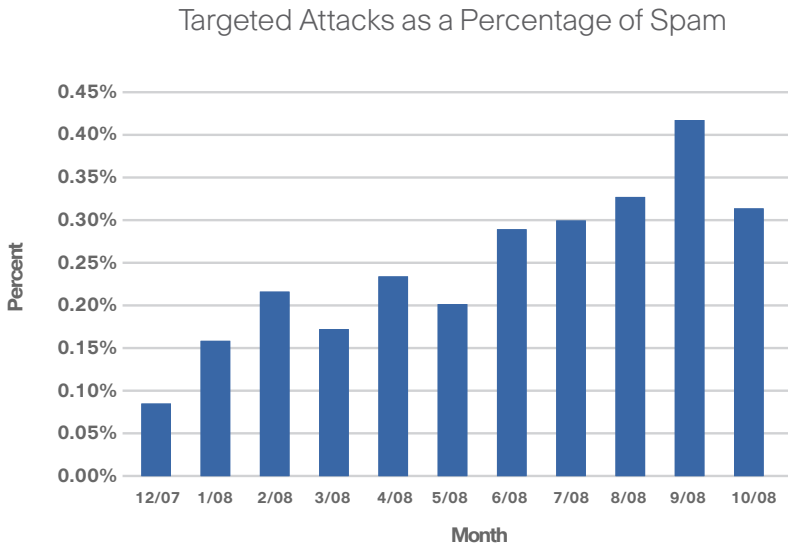
Unlike more common "mass" phishing emails, however, spear-phishing attacks rely on specific (usually stolen) information to craft a more personalized message—one the recipient is more likely to open and respond to. The personalized approach of spear phishing, combined with email reputation hijacking, in which criminals use a legitimate email provider's infrastructure to send messages, makes it more difficult to weed out these emails via standard anti-phishing technologies.

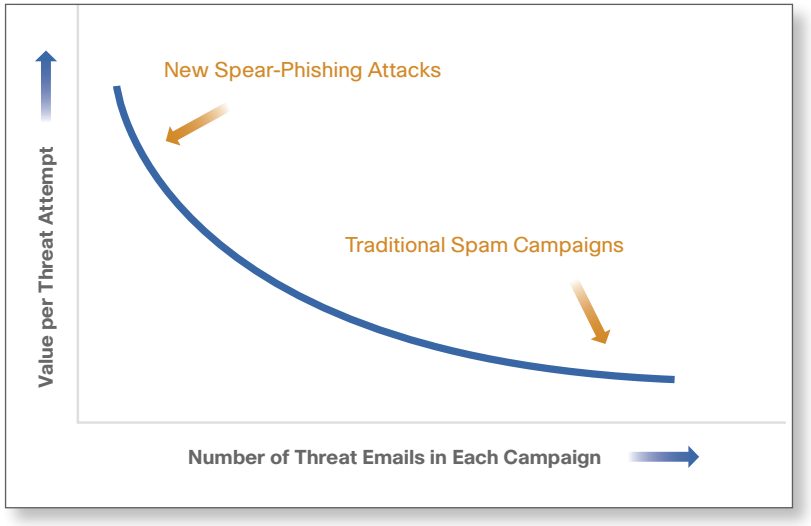
In many cases, online criminals rent or steal lists of valid email addresses, and can therefore personalize outgoing messages. Consequently, even savvy Internet users—conditioned to ignoring the less-sophisticated phishing messages sprayed to millions of people at the same time—can be lured into handing over login names, passwords, and other sensitive information.

For example, online criminals have been sending spear-phishing messages that appear to be from entities such as:

- The Internal Revenue Service, explaining that the recipient or the company is being audited.
- The Better Business Bureau, which has received a "complaint" about the recipient's company.
- U.S. district courts or tax courts, notifying recipients that they are being subpoenaed.

These messages look authentic and typically ask recipients to rapidly respond to the inquiry, which usually includes an attached "explanatory document." However, when opened, this file actually launches malware in the background to take control of the recipient's computer or network, or to install a keylogging program.





Spear-phishing campaigns are sent to fewer recipients, but are more likely to offer higher returns to criminals when recipients do respond to them.

Email Reputation Hijacking

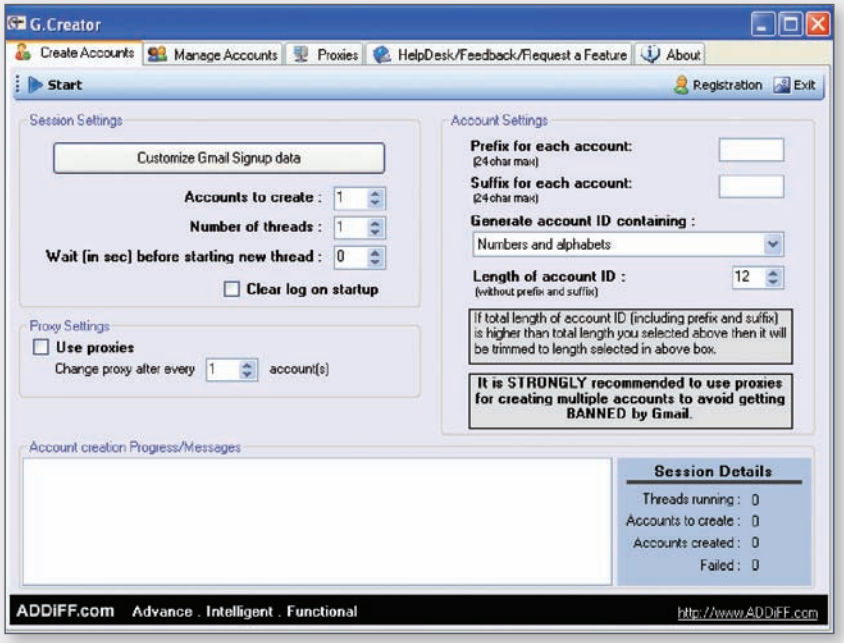
In email reputation hijacking, real email accounts with major legitimate webmail providers are used to send out spam. Taking advantage of the webmail provider's positive reputation offers increased deliverability: It makes the spam harder to detect and block, since it has the webmail provider's headers and formatting, and anti-spam solutions cannot block the mail servers of large webmail providers like Yahoo!, Gmail, and Hotmail.

The appeal of reputation hijacking has led to growth in the number of commercial tools available to spammers. These tools are aimed at making it simpler for spammers to create accounts, defeat CAPTCHAs, post, and rotate IP addresses to target webmail providers like Gmail, Yahoo!, and Hotmail, as well as sites like MySpace, Craigslist, and blogs.

Cisco estimates that during 2008, spam due to email reputation hijacking from the top three webmail providers—Microsoft, Gmail, and Yahoo!—accounted for just under one percent of all spam worldwide, but constituted 7.6 percent of all these providers' mail. The average spam rate from each webmail provider rose significantly for a period of time after tools to take advantage of their systems became available.

For example, in January 2008, Russian hacker "John Wane" defeated Yahoo!'s CAPTCHA. This led to an HTTP spike, followed by a three-month SMTP blitz. In May 2008, Google's CAPTCHA was broken, which led to an enormous spike in account creations. In August 2008, "John Wane" released AOL CAPTCHA-breaking code.

Email Reputation Hijacking Tools



Email reputation hijacking tools for the major webmail providers are commercially available and easily obtained. These tools were used frequently in 2008 and spam originating from these webmail providers increased significantly.

Data Loss

Despite best efforts, security incidents related to data loss are on the rise. Data loss can occur because of the physical loss or theft of systems and storage devices or the accidental sharing of information in an insecure fashion. Online criminals are using malware to steal consumer and company data online. Hackers are also getting their hands on data by breaking into insecure or weak systems and devices. And sometimes, insiders are the culprits.

More and more businesses are recognizing that their data is a precious asset that must be protected. PricewaterhouseCoopers' *2008 Global State of Information Security Study* reports that many more organizations are encrypting "sensitive information not just in laptops, but also in databases, file shares, backup tapes, and removable media." And many have made "significant strides in advancing Web/Internet capabilities," including content filters, website certification/accreditation, and secure browsers. The report also cites increased use of technologies that help protect wireless devices, and tools that can discover unauthorized devices or prevent intrusions.

According to the Privacy Rights Clearinghouse's *Chronology of Data Breaches*, since January 2005, more than 230 million records have been compromised due to security breaches. Cisco research shows that inadequate data security can have significant consequences for organizations, including business disruption, reduced productivity, and increased operational expenses—and those are on top of the obvious loss of sensitive data.

Data loss related to the loss or theft of equipment is an enormous problem for businesses and individual users. Ponemon Institute recently reported that the number of lost laptops at some medium-sized and large airports has been reaching more than 600,000 annually. More than half of the laptops are never reclaimed, as many people hold no hope their laptop will be found. Therefore, they often do not bother taking any steps to attempt to locate and retrieve them.

The following incidents that occurred in 2008 are related *just* to laptops:

- A laptop computer containing personal information—including names, addresses, and employee identification numbers—for approximately 13,000 workers of a global pharmaceutical company was stolen from an employee's car. The laptop was encrypted, but the flash drive was not; the latter contained potentially sensitive business information, according to a company spokesperson.
- In the summer of 2008, Verified Identity Pass (VIP), a vendor of the U.S. Transportation Security Administration that operates a Registered Traveler program under the brand Clear, temporarily misplaced a laptop that had been reportedly locked in an office at San Francisco International Airport. The laptop contained unencrypted personal information for 33,000 customers, but according to the vendor, none of the data was compromised.
- The U.S. Veterans Affairs (VA) Department, which suffered severe embarrassment in 2006 when a laptop containing millions of veterans' records was stolen, had its new security policies put to the test in spring 2008, when another of its laptops was stolen from an employee's Texas apartment. This time, the data was encrypted, no one without proper authentication could access the computer, and the VA knew which piece of equipment was missing. The employee also did his part by immediately reporting the theft to the VA and local authorities.
- The U.K.'s Ministry of Defense reported a serious breach of security when a laptop containing unencrypted data related to 600,000 prospective military recruits, including some financial and passport information and medical details, was stolen from a military recruitment officer's car.

Fortunately, very few incidents of equipment loss or theft result in information being passed on to criminals with the expertise to profit from accessing and using the compromised data. These are usually simple thefts, with the end goal of quickly reselling the equipment, which is wiped clean of data to conceal the fact it has been stolen.

Data Loss Issues on the Regulatory Radar

Data breach notification legislation now requires that companies report when sensitive data is potentially lost—such as when a laptop is stolen.

Currently, 42 U.S. states and the District of Columbia have data breach notification laws on the books, or legislation pending approval. While state laws vary, they generally follow the California Security Breach Information Act (SB-1386), which requires organizations that electronically store personal data about customers to inform those individuals if the company knows the security of that information has been compromised.

Meanwhile, the U.S. government is attempting to address these notifications at the federal level and consolidate the variances in state laws—perhaps even strengthening some laws. It is also trying to align federal legislation with approved or pending legislation in other countries.

In addition, there are increasing laws and regulations to handle the sharing of sensitive data. New U.S. compliance regulations and market-driven industry best practices were released in 2008 that attempt to focus on stronger protection and increased enforcement for data loss violations. The federal government released the Red Flags provision of the new Fair and Accurate Credit Transactions Act, which spans multiple industries and requires businesses that provide services before billing to implement an identity theft prevention program. The initial enforcement period was November 2008, but it has been delayed to May 1, 2009.

In October 2008, the state of California passed two privacy laws, SB-541 and AB-211, that attempt to augment existing medical privacy compliance regulations by focusing on the enforcement of unauthorized access to patient health information, negligent disclosure of patient records, and illegal use of medical information for financial gain. The Health Information Trust Alliance will also release the HITRUST Common Security Framework (a market-driven

best practice) in January 2009. This framework is built upon industry standards such as ISO 2700x, B/S 7799, PCI, and the NIST 800 series.

Individual U.S. states are also imposing their own laws to mandate encryption of personal information sent over the Internet by businesses located in the state. New laws and regulations require, among other things, encryption of personal information on laptops, PDAs, and portable media (including flash drives); encryption of personal information transmitted over the Internet; development and publication of Social Security number (SSN) privacy protection policies; and specific measures to protect the confidentiality and security of employee SSNs.

While such legislation obviously benefits those whose data has been compromised, disclosing a security breach may leave an organization subject to negative media coverage and possibly cause long-term reputation damage. This can lead to a drop in the confidence of users and customers, who may be inclined to take their business elsewhere.

Many laws and regulations carry significant statutory penalties for violations as well as the possibility of businesses facing private rights of action for noncompliance. As a result, an increasing number of businesses are using encryption and other access control technologies to help ensure compliance.

The Limitations of Compliance

While many regulatory standards attempt to help protect user data, compliance cannot be a security placebo. Many companies have made great strides to achieve compliance measures, but the sense of urgency that often surrounds compliance demands should not become a distraction from other, crucial threats to security. By focusing almost exclusively on compliance and aligning procedures to meet those requirements, organizations can lose sight of the rapidly evolving risk and threat environment. In fact, multiple security incidents in 2008 involved organizations that were considered "compliant," but were compromised by exploits not covered by compliance requirements. Many compliance procedures do not and cannot address today's array of applications, technologies, tools, and the related security vulnerabilities that are increasingly being targeted by threats. Instead, compliance measures are intended to help organizations achieve specific objectives that mitigate only *certain* security risks.

The market-driven Payment Card Industry Data Security Standard (PCI DSS), for example, focuses on the protection of cardholder data during processing, transmission, or storage. It is a detailed standard compared to other compliance regulations. However, it does not entirely mandate a strong level of security, as it must balance its strict requirements with a risk-based approach that can apply to both small and large organizations. The industry recently updated PCI DSS to version 1.2. In addition to merging both versions of the requirements and testing validation steps, the revised standard provides new deadlines around Wired Equivalent Privacy (WEP) replacement and adopts a risk-based analysis approach so to help smaller businesses comply.

To address the array of compliance best practices and regulations, organizations will likely plan larger IT governance, risk management, and compliance (GRC) programs. Although achieving compliance is important, organizations must remember that many best practices and regulations apply only to protecting certain information—for example, company financial information (Sarbanes-Oxley), patient medical information (HIPAA), and personally identifiable information (Basel II, and U.K. and EU data laws). Therefore, in addition to regular compliance reviews, organizations will often conduct top-down gap analyses to improve existing procedures and proactively meet current and emerging threats.

Recycling Risks

Recycling of electronics equipment is becoming more common. In fact, some countries already charge buyers a recycling fee when they purchase any electronics item. All or part of that fee may be reimbursed if, at the end of its useful life, the item is taken or sent to a recycling center. Organizations—looking to recoup those fees, comply with laws and regulations, or simply be more environmentally responsible—are likely to recycle more often. Yet while more organizations are recycling their "e-waste," many aren't taking sufficient precautions to make sure those items have been wiped clean of sensitive data.

Once equipment destined for recycling is sent away, there is no telling where it may go or what will happen to any data that can be extracted from it. Press reports indicate that some devices have ended up as far afield as Indonesia and West Africa, where salvaged data is sold at bargain-basement prices.

Many organizations do not make the IT department responsible for (or at least involved in) the electronics equipment recycling process, instead leaving it to other departments, such as facilities management. However, it is unlikely that personnel outside of IT will be aware of the importance of degaussing hard drives and otherwise safeguarding potentially sensitive data on defunct devices before those devices end up in a recycling facility. Consequently, organizations without clear, security-oriented policies for how to and who should handle this process within the organization may put sensitive data at risk.

Identity Theft

Identity theft continued to rise during 2008 and shows no signs of slowing down. Many online criminals have been successful at using social engineering tactics that feed on the trust of others, and allow sensitive personal data to be harvested, ranging from Social Security and driver's license numbers to complete medical histories.

Collating data from a variety of publicly available sources—including user profiles on popular social and professional networking sites—makes it easy to pull together enough information about a person's identity to create a scheme that either takes advantage of the individual, or of people who they know and who trust them.

For victims of identity theft, the risks have increased significantly: Just one security breach—whether it is keylogger malware invisibly downloaded to their home computer by a compromised website, or hackers cracking into the customer database of their favorite retailer thousands of miles away—can compromise their personal information.

And now, stolen personal information is being bundled and sold to criminal elements around the world—such as organized crime rings or even hostile governments. Those who tap this market use the information not only for profit, but also to sell to those who use the information for terrorism-related activities, such as creating fake passports and other travel documents, or laundering money for terrorist cells.

Targeting the Masses

Although the instances of highly targeted phishing campaigns are growing in number, most online criminals looking to commit identity theft are not going out of their way to target specific individuals or groups—at least, not yet. They are simply trying to snare as many people as possible.

The Internet provides ample opportunities for identity thieves looking to target the masses. According to a report released by the FTC in February 2008, some 64 percent of fraud complaints in 2007 related to incidents where the method of initial contact was an Internet solicitation, such as email.

The economic impact to individuals who are victims of identity theft is obvious. But businesses also suffer in terms of reputation damage and financial loss, particularly in instances when the trust of many consumers has been compromised. For example, sophisticated phishing techniques can dupe users into believing they are interacting with a trusted source—such as an individual, charity organization, bank, or online retailer—via spam emails and with legitimate-looking but fake websites.

Other data-gathering opportunities for today's identity thieves include:

- **Social networking**—A rich trove of personal information, including phone numbers, addresses, full names, and birthdates, is available on user profiles posted on social networking sites such as Facebook and MySpace, and additional personal information such as mothers' maiden names on sites like Ancestry.com.
- **File sharing and peer-to-peer software**—When users allow friends and associates to access certain files, such as MP3s, other files on their computers can be easily compromised. "Access creep" is also a growing problem in collaborative work environments, with people being allowed to view too much information, including company secrets and information about coworkers.
- **RFID tags**—Some concealable readers can read radio frequency identification (RFID) tags from a short distance (up to a few feet) to gather data from credit and other types of cards. RFID tags can be cloned, and the equipment required to do this is available. This has clear security threat implications: RFID technology is used in everything from building access cards to passports.

Rethinking Identity Management

Given the concerns around data loss and identity theft, the recent resurgence of interest in identity management is not surprising. Many leading companies are overhauling the security platforms they have long relied on and adopting new identity management technology. They look to prevent data loss, reduce the potential for identity theft, limit opportunities for insiders to engage in criminal activities, and comply with regulatory standards. They also require technology that supports collaboration among their remote workforce using Web 2.0 tools and applications, as well as with other organizations.

Today's identity management solutions have advanced well beyond easy-to-compromise usernames and passwords required to access networks or applications. Secure, personalized user profiles may be created. And before access is approved, users may have to be verified through one or more methods, including tokens or smart cards. Some organizations use biometrics, including fingerprints and iris scans, to authenticate users.

Transparency is another theme in modern identity management. Organizations want technology that allows them to monitor user activities from sign-on to sign-off. They need solutions designed to set boundaries on the amount and types of information and other resources users are permitted to access. In addition to making it easier to track user activity, identity management technologies now on the market allow organizations to set consistent user policies and conduct auditing and reporting to help assure compliance with regulatory standards.

There is strong demand for identity management solutions that are complete and highly effective but also easy to use. That's why more organizations are looking to "single sign-on" solutions that simplify the process of verifying user identity and give users access to the information and applications they need. But while identity management technology has advanced dramatically in recent years, the industry continues working on developing solutions that provide even greater security and user monitoring capabilities—and don't hinder workforce productivity.

The Human Factor

People are still the weakest link in the security chain. But their capacity to learn and modify their behavior in response to information means they also represent an area with a great opportunity for improvement. Attacks on websites and corporate networks continue to increase in sophistication, and online criminals are growing proficient at duping even the savviest or most cautious of users.

Human Nature Invites Risk

Plain and simple human error—such as a CEO opening an email that appears to be from a trusted source, but is really a well-disguised "whaling" attack, or poor judgment, such as engaging in e-commerce on a website that does not have a valid security certificate and is a front for a scam—is often what triggers the release of malicious attacks or leads to identity theft and other fraud.

Human carelessness—for example, losing an employer-issued laptop or inadvertently posting a company's sensitive information on a blog—can also quickly turn into a reputation-damaging event, and cause significant financial loss for an organization. Email address errors are another common human mistake-based security problem that can easily result in highly sensitive information being sent to the wrong people.

Even the security-conscious U.S. military is not immune to such blunders: In 2008, it was reported that United States Air Force (USAF) personnel inadvertently sent email messages intended for USAF personnel stationed at Royal Air Force Base RAF Mildenhall in Suffolk, England, to a tourist website with a similar email address. The maintainer of that site, which is intended to promote tourism in Mildenhall, notified the USAF several times about the emails but was told not to be concerned. Only when officials were notified that flight plans for a presidential visit were received did they become—reactively—alarmed.

Technology solutions (such as anti-spam tools and outgoing email monitoring) can be helpful for proactively mitigating some risks and preventing widespread damage from certain types of attacks. Providing ongoing threat education and training for employees—and building their awareness about security risks and the importance of safeguarding data—remain important security defense measures for organizations. But they have their limitations. Technology can create a false sense of safety, and neither that or education can address a broader security problem: human nature.

By nature, most people are curious, eager to communicate, and interested in good deals or attractive "freebies." Quite often, they also are overconfident that *they* are not the type of people who would fall prey to trickery or scams; this aspect of human behavior is a key element in making online crime work.

Online criminals thrive by taking advantage of Internet users' trust and human nature. Countless people continue to be lured to malware-distributing or phishing websites by emails containing URLs. Given that more than 80 percent of spam messages now contain URLs, it is not difficult to see why this hit-or-miss approach succeeds. And with potent and self-propagating malware available, even a relatively small number of infected users can infect many more.

Remote Working, Social Networking: Opportunities and Risks

Having a mobile workforce can significantly improve business productivity, and keep workers happy by allowing for better life-work balance. A global workforce can be very cost-effective, allowing for localized service to customers in different regions and faster entry into new markets. And many workers today (especially young, highly wired "Generation Y" workers) love using new tools and technologies that make work and life easier and more fun.

Organizations are equipping their remote workforces with the collaborative tools and mobile devices they need to do business anywhere, anytime. But by doing so, they also create security risks. For example, in its *Emerging Cyber Threats Report for 2009*, Georgia Tech Information Security Center warns that as Internet telephony and mobile computing—which are essential to remote workers—handle more and more data, they will become more frequent targets of online crime. The report predicts that criminals will be "drawn to the VoIP medium to engage in voice fraud, data theft, and other scams—similar to the problems email has experienced."

Meanwhile, the line between technology use for personal and professional purposes is becoming increasingly blurred. Recent Cisco research revealed that 44 percent of employees share work devices with others without supervision, and 46 percent said they transferred files between work and personal computers when working at home.

A report by Telework Exchange and Sprint Nextel on wireless Internet usage among U.S. government employees revealed that 33 percent of teleworkers, and 11 percent of IT workers, were not familiar with security guidelines for using wireless Internet.

Cisco's recent research into security perceptions and online behavior of remote workers in several countries (including Brazil, France, India, and the United States) showed that using work computers and devices for personal use is a widely accepted practice today. A primary reason for this casual attitude cited by survey respondents: The belief that their employer does not mind. What's more, many users download certain tools and applications in an effort to be more efficient in their jobs, but can wind up derailing overall productivity by unknowingly creating a convenient inroad for a threat.

Elements of human nature, such as being curious and having the desire to connect with others, also create risk for organizations, which can expect more of their employees (mobile or otherwise) to engage in social and professional networking online while on the job. Some companies are encouraging this activity—using such outlets for their own marketing, PR, and HR initiatives. Even the microblogging utility Twitter is now being used by leading companies to share product news and offer special deals to those who sign up for the service.

Providing proactive and thorough user education, and setting clear policies about social networking and other online activities while at work, is good practice. However, many organizations either fail to set appropriate use policies or do not communicate them to users or internal resources expected to help enforce such practices. A report by Telework Exchange and Sprint Nextel on wireless Internet usage among U.S. government employees revealed that 33 percent of teleworkers, and 11 percent of IT workers, were not familiar with security guidelines for using wireless Internet.

Inadequate or insufficiently communicated appropriate use policies will have to change. With popular sites such as MySpace and Facebook likely to remain highly vulnerable to hard-to-detect malware such as Koobface, organizations will need to pay more attention to on-the-job social networking by employees. Koobface works to turns infected users' computers into botnet nodes. The worm searches for cookies associated with a social networking site and, once located, modifies them and embeds malicious links on a user's profile. Others viewing the profile assume the links were put there by the user. Trusting the source, they click on the links and also become infected with malware. (Instructing workers to clear their cookies on a daily basis can help combat this problem.)

Meanwhile, the laptops, mobile phones, PDAs, and data storage devices that both remote and onsite workers are using to engage in business and personal activities are providing myriad points of entry for spam, viruses, and malware. They also offer endless opportunities for loss of intellectual property and other data.

Workers may be insufficiently aware of the unprotected nature of mobile phones, the need to use privacy screens while doing sensitive work in public places, and taking extra care with easily misplaced mobile devices. A thumb drive can now contain as much as 64 GB of data, and the U.K. Ministry of Defense recently had to admit to several instances of sensitive information lost by officials moving data physically between locations, including a classified report on Al Qaeda, which was left on a train.

Using Social Networking and Web 2.0 Sites for Online and Offline Crime

Social networking websites such as Facebook, MySpace, Bebo, LinkedIn, Orkut (extremely popular in Brazil), and vKontakte (in Russia) have all been linked to spam and malware attacks. The Web 2.0 widgets and different types of potentially vulnerable content that users can add to their pages may make it especially easy for malware creators to exploit these websites in the year ahead.

Yet not all criminal uses of social networking and Web 2.0 sites take place exclusively online. Canadian and U.S. anti-fraud organizations reported a disturbing trend that surfaced in 2008: A sharp uptick in phone calls used in extortion schemes targeting senior citizens, which have resulted in victims paying thousands of dollars to criminals. The caller relays a fictional story about the senior's teenage or college-age grandchild needing to make bail in Canada—likely gathering personal information to use in the scam, such as the names of victims' grandchildren, from profiles posted on social networking and other Web 2.0 sites.

It also works the other way around, with online criminals "borrowing" elements from the physical world to help make their online scams appear credible.

Online scammers have been running so-called "419" (named after the section of the Nigerian penal code, where such scams often originate) or advance-fee fraud—a confidence trick that has been around for decades—on websites such as LinkedIn and Craigslist. A typical Craigslist scheme: The criminals use legitimate but outdated house-for-rent postings from other Craigslist users to dupe potential renters into wiring money to the "landlord," who claims he or she had to suddenly move overseas, and must rent out his or her house immediately—and cheaply.

In some cases where an address for the home is provided in the ad, victims have been told by the scammer that while a property tour was not available, they should drive by the house to have a look. While there may be plenty of red flags visible in retrospect, for many people seeing is believing, which is why this scam has been successful.

In another recent social engineering scheme involving Craigslist, a resourceful bank robber enlisted "help" for a robbery getaway through false advertising. The suspect posted a listing on the site advertising a road maintenance project that would pay US$28.50 per hour. Around a dozen unsuspecting decoys-to-be who applied were asked to show up for work at a local bank wearing specific attire—a yellow vest, safety goggles, a respirator mask and, if possible, a blue shirt.

They did as instructed, but when they arrived at the jobsite they found no work to be done and no contractor. At the same time, the robber (wearing the same gear as the decoys) wrestled a bag of cash from an armored truck guard and made a clean getaway—leaving the police to sort through a dozen look-alike suspects.

Insider Threats

External threats such as Web-based malware and hacker intrusions may be more numerous, but organizations should never ignore the significant security risks posed by insiders. Insider threats can be even more damaging to a company's reputation and financial well-being than ones that originate outside the organization.

Adding to concerns about insider threats, larger entities such as competing corporations and hostile governments (as well as organized crime) have been placing agents within organizations they wish to compromise. The extreme volatility and deep uncertainty felt throughout the global economy in the latter half of 2008—which will likely carry well into 2009—is another reason why insider threats can be expected to remain a major security concern for businesses of all types.

This year saw a rise worldwide in the number of instances of fraud, hacking, and identity theft by insiders—or those who were able to compromise physical security controls to gain access to an organization's networks. Underscoring this trend are the following incidents reported in the past year that were not discovered until after significant financial damage had occurred:

- In January 2008, a trader for French bank Société Générale admitted that by engaging in unauthorized stock market deals, he had caused a €4.9 billion loss for the financial institution. The employee used knowledge and experience he'd gained through previous work in the bank's risk management office to conceal his losses through falsified transactions.

  The trader's fraudulent activity—which required a breach of five layers of control and included the theft of computer access codes—was discovered by auditors looking into an error made by the bank's chairman and CEO. It is believed this trader acted alone, and was motivated not only by the desire for personal gain, but to enhance his trading reputation within the organization.

- In May 2008, three men (with direct access to the hardware targeted in the crime) were charged with hacking into 11 cash register terminals and stealing credit and debit card numbers from customers at a popular U.S. restaurant chain. A "packet sniffer"—a computer code designed to capture communication between computer systems on a single network—was installed on point-of-sale servers at the targeted restaurants. Over the course of seven months in 2007, data was collected from thousands of credit and debit cards. At just one location, more than 5000 cards were compromised, resulting in at least US$600,000 in losses for the financial institutions which issued the cards.

- There was even more bad news for the U.S. mortgage industry in 2008 when an investigation of mortgage brokers in the state of Florida, conducted by *The Miami Herald*, revealed that thousands of licensed brokers had criminal records that should have been discovered during mandatory background checks. Regulators must approve licenses for mortgage brokers in Florida, where background checks have been required since 2006. According to the newspaper's report, more than 10,500 people with criminal records were approved to work in the mortgage profession.

  The investigation uncovered an estimated US$85 million in losses due to fraud, identity theft, and theft of savings and homes involving licensed brokers. In addition, several brokers who committed fraud were—remarkably—allowed by regulators to keep their license. With public records and the current technologies available to anyone with an Internet connection, conducting background checks is a relatively simple, inexpensive, and quick control that can identify potential security issues.

- In October 2008, an onsite IT contractor for Shell Oil was caught stealing information about current and former U.S.-based employees from a company database. According to Shell, the contractor used Social Security numbers belonging to four employees to file fraudulent unemployment claims. After discovering the breach, Shell had the contractor removed from the premises. The company dropped its contract with the associated vendor and alerted its employees of the breach. The Texas Workforce Commission and local law enforcement are investigating the incident.

Financial Crisis May Heighten Insider Risk

Due to the global financial downturn, Gartner analysts are predicting large IT budget cuts as well as hiring freezes and layoffs. If workforces are to be cut in response to the financial pinch being felt by many organizations, many employees could become "disgruntled about-to-be-ex-employees." And disgruntled employees could offer many opportunities for online criminals to gain access to sensitive data, passwords, and the IT infrastructure.

For instance, consider the World Bank. According to some reports, an IT consultant infected the computers of several coworkers with keylogging software, gaining the ability to compromise several of its servers. As of mid-October 2008, the World Bank denies that sensitive information was compromised, but this story showcases the vulnerability of institutions and organizations that were otherwise perceived as robust and trustworthy.

With many companies globalizing their workforces, we are increasingly living in a single, integrated world economy. Employees of American banks and IT firms may be working out of call centers in Asia or Europe. Making sure the security policies put in place are usable in the context of local culture, but also work within the global security policies of a multinational organization, is crucial. In addition, as companies cut costs they may increase their dependence on teleworkers and consultants. This can be cost-effective, but requires additional security policies and implementations to work securely at the edges of an organization's network.

Issues of Trust

Many users believe they enjoy the same levels of data security they enjoyed in the past, when transactions and related data existed primarily in the physical realm. They trust that organizations they willingly give their personal information to will do everything possible to safeguard it. And they believe the equipment and services of providers they know and trust are secure.

Users can put their information at risk of exposure in more ways than ever before, whether by tapping into a local coffee shop's unsecured Wi-Fi network (easily sniffed by identity thieves) or making a purchase from a national retailer that relies on archaic data storage methods (easily compromised by hackers).

Organizations can be just as naïve about their own security. They may put too much trust in existing protocols, services, and components, or may not do enough to validate and monitor trusted relationships through available methods such as certificates, monitoring, and testing. Meanwhile, some businesses compliant with certain regulatory or industry standards assume meeting these standards ensures adequate security.

Ignoring known weaknesses is another problem for organizations. Consider that much of what was "new" in the way of threats during 2008 essentially came down to online criminals exploiting old problems—unpatched systems, weak security policies, and known vulnerabilities in the core infrastructure of the Web. By not addressing and patching existing issues, organizations cannot adequately prepare to combat new threats.

The threat against network operating systems has grown substantially over the past decade and recently, there has been a notable surge in criminal activity related to the exploitation of fragile networks. To fortify the networking and IT systems that make up their critical infrastructure, many organizations are now making such upgrades a part of their security strategy. In fact, some are viewing annual upgrades as being only a bare-minimum effort, and are conducting upgrades twice a year or more.

Another ongoing risk for organizations is people. For instance, employees can lose equipment, which can compromise sensitive data. Insiders looking to commit fraud also have more incentive today: The increase in data density makes attacks originating from within an organization much more profitable. Properly placed devices designed to sniff or collect sensitive data, or the copying of data that an employee has legitimate access to, are known to be at the root of several of 2008's high-profile security incidents.

Even hardware can pose a threat: Counterfeit chips inserted into computer equipment can obviously put sensitive data of individual users, businesses, and governments at risk. It may sound like fodder for a spy novel, but there have been reports of criminals (and even foreign governments) finding opportunities along the global supply chain to embed counterfeit components into devices.

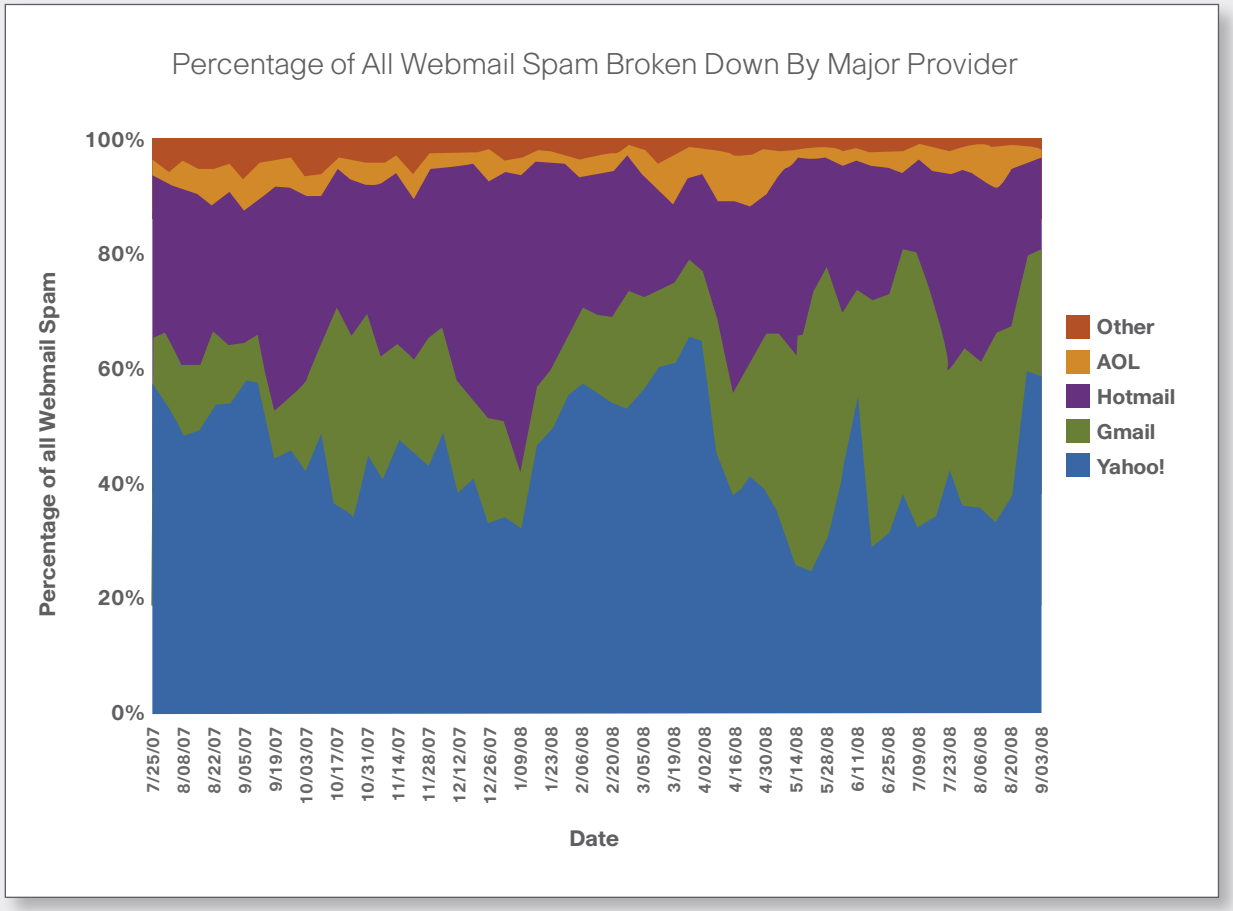
While some experts say the security threat is overblown, counterfeit components can provide the "back door" that external parties need to access a user's personal information or monitor their communication. They are also extremely difficult to detect and can be costly to address. While software can be patched, counterfeit components must be removed one machine at a time.

Ignoring known weaknesses is another problem for organizations. By not addressing and patching existing issues, organizations cannot adequately prepare to combat new threats.

New Tactics Erode Trust

Online criminals look for any and all favorable tactics to take advantage of users' trust—hence, the growing popularity of various kinds of reputation hijacking. In 2008, many leading companies with well-known and trusted brands had their reputations compromised by these attacks. Criminals successfully hijacked reputations by:

- Creating highly credible spam that appeared to come from a real company—both visually and by spoofing header information. Recipients were directed to legitimate-looking websites that were clever fakes.
- Overcoming security measures designed to avoid the mass creation of webmail accounts from top webmail providers with trusted reputations. Once criminals gained the ability to create large quantities of webmail accounts, they used them to send out massive amounts of spam, which was more likely to get through anti-spam filtering systems due to the legitimate webmail sender address.
- Poisoning DNS caches from local Internet providers so that typing in the legitimate URL would lead to a malicious site where users would provide sensitive personal and financial information.
- Inserting malware-downloading iFrames into thousands of legitimate websites (including those of major retailers and news organizations) through SQL injection and cross-site scripting, among other methods. A recent Cisco study estimates that 20 percent of all legitimate sites have been tainted by this type of attack.



The average spam rate from each webmail provider rose significantly for a period of time after tools to take advantage of their systems became commercially available.

Privacy and Trust Violations

More consumers are learning that their privacy may not be well protected by sources they trust. Businesses and organizations are freely sharing consumer information with third parties for advertising and marketing purposes. Often, they do not disclose that fact to consumers (or at least not as clearly as they should). Even when they do spell out policies, users may not read them (thoroughly or at all) before clicking "accept."

Sometimes, consumer data is put at risk when everyone in an organization does not fully understand the privacy protection practices, or when third-party vendors trusted with sensitive information are not aware of or do not follow security policies.

IT and privacy departments that establish strict policies around the use of customer data may find other departments undermining those directives. A 2008 Ponemon Institute study of executives shows that security and privacy officers responsible for protecting consumer data gathered by their organizations are clearly at odds with their own marketing departments, which share the same data (including email addresses) with external parties.

Universities, for example, gather and maintain a large amount of detailed personal and financial information related to their students and alumni. Last year, it came to light that many universities have been sharing this information with outside companies, including banks and credit card providers—a practice often in direct opposition to privacy protection policies, statements, and information provided directly to students.

Florida State University recently came under fire for providing names and addresses of students and alumni to Bank of America for a credit card promotion. The Consumer Warning Network (which obtained a copy of the contract) uncovered that, as part of the deal, the university receives a portion of every dollar charged by students and alumni on the credit cards, which feature the school's colors and logo. Florida State University reportedly is guaranteed to receive US$10 million over several years, and the money is being paid directly to the Seminole Boosters, a private entity that raises funds to support the school's athletic program—including paying coaches' salaries.

The irony of this situation: While doing this deal with Bank of America, Florida State University was simultaneously engaged in a media campaign warning its students of the dangers of credit card debt.

Vulnerabilities

Vulnerabilities exist in many technologies. Criminals take advantage of these weaknesses to install malware on computers and devices, gain control of computers and networks, and profit by making them parts of botnets or stealing sensitive data stored on them.

To lower the risks of having criminals gain control over their systems, IT professionals and individual users work to find patches, fixes, and upgrades for the products and systems they use. It can look like a race between criminals looking for new or more attractive vulnerabilities to exploit and users trying to keep their systems patched and as secure as possible.

However, it can sometimes feel onerous to users to find and install patches or deal with the hassle of upgrading, and they may fall behind in keeping their systems and products patched and upgraded. This can be a real boon for criminals, as certain longstanding but not-always-patched vulnerabilities can offer easy ways of infiltrating systems.

The types of vulnerabilities most often exploited have changed over the years. Certain vulnerabilities are now more likely to be patched (sometimes automatically) as vendors have developed systems to both disclose and release patches for them.

In fact, Cisco found that the number of reported vulnerabilities in 2008 increased compared to 2007, growing by 11.5 percent. This continues the trend of previous years, and shows that vendors are more actively reviewing, identifying, and correcting vulnerabilities in their products. They're also more often collaborating with security researchers to do so.

According to the July 2008 IBM *Internet Security Systems X-Force Trend Statistics* report, security research organizations are finding nearly 80 percent of critical vulnerabilities. This correlates with Cisco information, which indicates that around 80 percent of critical vulnerability disclosures are coordinated with vendors of the affected products so that they can release patches or updates at the time of disclosure.

One result is that, while the overall number of disclosed vulnerabilities is rising, the number of "zero-day" vulnerabilities (vulnerabilities for which there is no patch available when exploit code is made public or discovered in the wild) in products such as major operating systems seems to be declining.

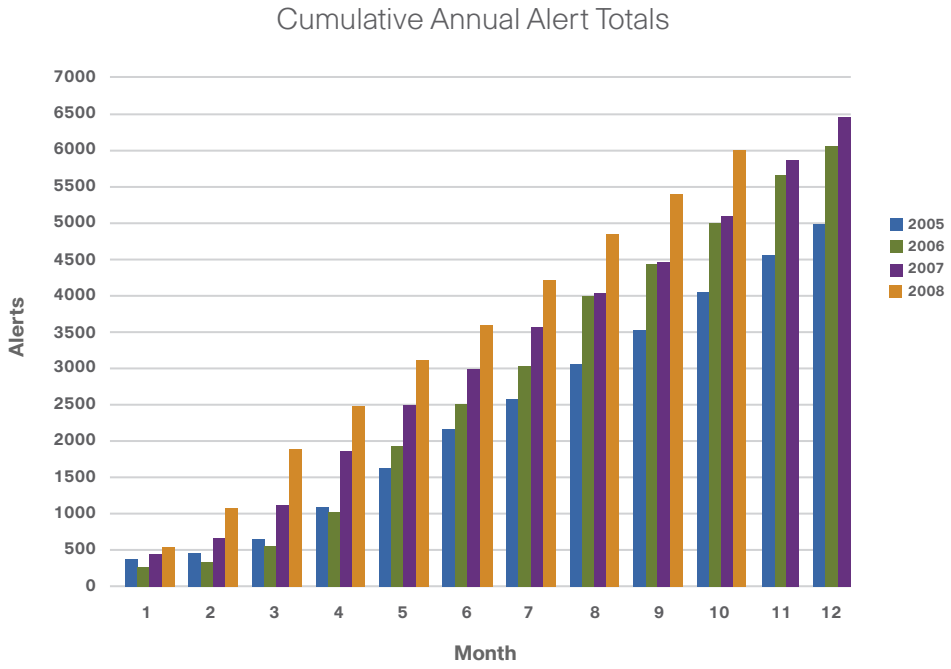
Another vulnerability trend is that many attacks now use a combination of multiple exploits that each target different weaknesses to increase the attack's access and control of the system. These combinations used in cross-vulnerability attacks can vary widely, depending on what operating system and programs are running on the targeted system.

Web Vulnerabilities

With the Web being used by more people for more purposes in more new, untested ways, vulnerabilities along the entire Web ecosystem—including browsers, Web applications running in those browsers, servers, and some of the underlying infrastructure of the Web—continue to grow in number and importance.

And it's not just that new ways of use are creating new vulnerabilities. Many known vulnerabilities in Web-based tools and technologies continue to be exploited by online criminals. Some high-profile Web-based technologies known to have vulnerabilities include:

Adobe Flash Player. When users click on and view a malicious Flash file on a website or in an email, this can trigger the execution of arbitrary code with the privileges



The number of reported vulnerabilities in 2008 increased compared to 2007, growing by 11.5 percent.

of the user. If the user is logged on to their computer with an admin account, the attacker could execute code that completely compromises the system. Widespread attacks using this vulnerability were conducted in April and May 2008. Adobe released updated Flash Player software in response, and multiple vendors updated their security settings and tools to stop this exploit.

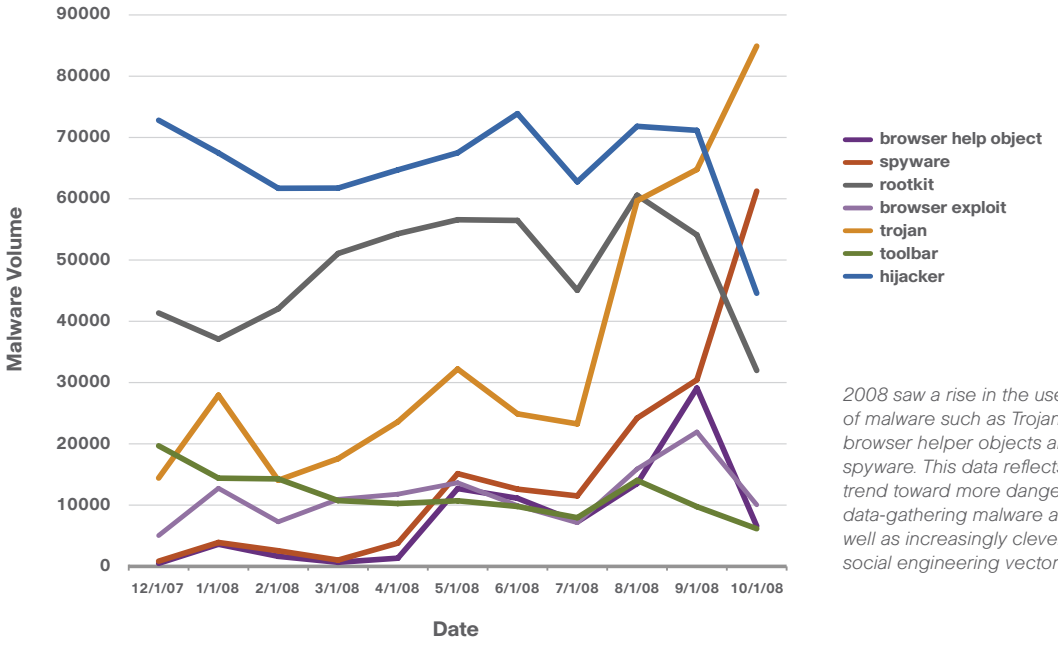
WordPress. In March 2007, an entire version of this widely used blog-creation software was compromised when online criminals gained user-level access to a server hosting the latest official release of the software. They inserted malicious code into the then-latest official release. Anyone who downloaded and installed that version during the days it was up on the site ended up making their blog vulnerable to remote PHP execution by online criminals. In response, WordPress released a new version and hardened its servers.

Media players. Many popular media players used to play multimedia content that is either downloaded from the Internet or embedded in webpages have proven to be vulnerable to exploits. Vulnerable players include RealPlayer, Windows Media Player, Adobe Flash Player, and QuickTime. For online criminals, media players can be especially attractive to try to compromise, since users are conditioned to receiving messages that they should upgrade their media player to be able to play different kinds of content or for security. Sometimes these messages are legitimate, and may be ignored due to being viewed as a hassle, leaving the player vulnerable; other times these messages are attempts to exploit the media player to install malware on the user's computer.

"With the increased complexity of many systems, entire classes of vulnerabilities can start to combine, so that individual vulnerabilities that may have seemed relatively harmless alone can turn into a serious risk factor when partnered with other threats."

—Greg Spillman, Cisco Security Analyst

Different Types of Malware Detected (by month)



2008 saw a rise in the use of malware such as Trojans, browser helper objects and spyware. This data reflects a trend toward more dangerous, data-gathering malware as well as increasingly clever social engineering vectors.

Besides these well-known Web-based technologies that have proven to be vulnerable to attack, the growing crop of new Web 2.0 technologies such as widgets and add-ons for blogs and social networking sites may also be vulnerable.

There is also the risk that not all of these add-ons are well-intentioned. Developers have already been creating malware distribution, management, and support packages. Social engineering continues to be widely used by online criminals, many of whom have become aware of the value of social networks. Therefore, it seems logical that some of these developers would turn their attention to creating custom, highly appealing "mal-widgets" for social networking sites.

ActiveX Vulnerabilities

Vulnerabilities in ActiveX controls, which power many Microsoft applications and Windows applications, including the widely used Internet Explorer Web browser, continue to appear in very large numbers. Exploiting these vulnerabilities typically involves convincing a user to visit a malicious website that invokes a vulnerable ActiveX control.

Attackers used vulnerabilities in the Microsoft Snapshot Viewer, RealNetworks RealPlayer, Microsoft Help Visuals, and Computer Associates BrightStor ARCserve Backup ActiveX controls to conduct high-profile attacks in 2008. ActiveX vulnerabilities have also been used to propagate malware such as that which targeted outdated versions of RealNetworks RealPlayer for Windows. As evidenced by its success, users often have outdated versions of ActiveX controls installed. As in many situations, even though the vendor released an update to resolve the vulnerability, many users hadn't updated the software.

DNS Vulnerabilities

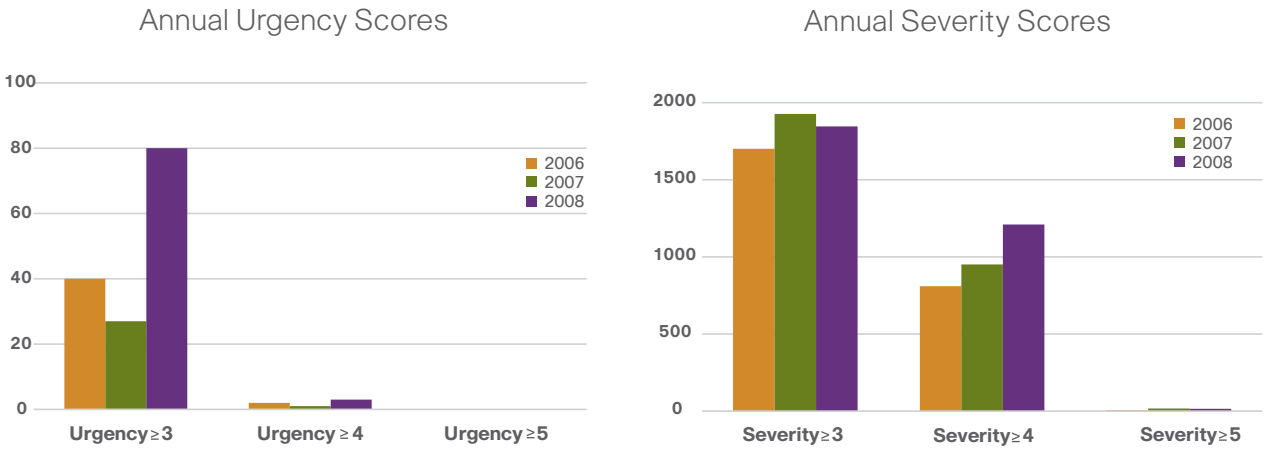
The big online security concern of 2008 may have been a Web ecosystem vulnerability that received extensive news coverage at the end of the summer. It involved vulnerabilities in a critical part of the Web's infrastructure, the Domain Name System (DNS) protocol.

The function of the DNS protocol is to resolve URLs and hostnames such as "cisco.com" to their numerical IP addresses, or IP addresses to URLs. The DNS protocol allows users to find websites by typing in "http://www.cisco.com" rather than "http://198.133.219.25". This makes it easy to associate domains and related subdomains with each other, even if the servers they are hosted on are not physically near each other.

DNS servers keep records of which domain names go with which IP addresses. When a DNS server receives a request to resolve a domain name in an IP address from a DNS client, it can look into the portion of the global DNS database it manages, or it can relay the query to other DNS servers that manage other portions of the global DNS database. To speed up their response time, DNS servers locally store responses they receive from other DNS servers in a local cache for a certain amount of time.

In an attempt to evade being blocked by IP address blacklists, botnet operators and other online criminals often take advantage of the DNS server's lack of restrictions on how frequently the records of a domain name and its associated IP address can be changed. Every few minutes, the malsite operators transfer the task of hosting a malsite from one botnet node to another. This practice is called "fast-flux," or domain-name kiting.

Worse, the DNS protocol itself—not just the lack of restrictions around changing the records in the DNS—has been shown to have exploitable vulnerabilities in the area of "cache poisoning."



These graphs show that both the urgency of vulnerabilities and threats (which is the equivalent of activity) and the severity (equal to the impact) are continuing to increase.

Recent Attacks Using DNS Cache Poisoning

China Netcom. DNS cache poisoning claimed one of China's largest ISPs, China Netcom, as a victim. The online criminals who poisoned the DNS cache worked to stay low-profile, limiting the URLs they redirected to malicious websites to those misspelled by users attempting to visit certain legitimate websites. This limited the number of victims, but made the attack sneakier and presumably slower to detect.

AT&T Internet Services. A DNS server resolving DNS queries for customers of AT&T Internet Services (formerly SBC) in the area of Austin, Texas, was compromised. It redirected AT&T Internet Services customers who tried to visit google.com to a malicious page that showed a fake version of the Google page and incorporated iFrame exploits.

The Importance of DNS

Almost everything the Internet is used for—not just the Web, but also email, FTP, voice over IP, banking transactions, and more—relies on the DNS. The DNS acts as the master map of the Internet. Users assume that map is correct, but if criminals can modify copies of that map, they can send anyone using that copy of the map (the DNS cache) to a completely unexpected destination, even while the users are being shown that they're following the map to their desired destination.

This is an especially crucial issue because the DNS is built to be distributed, with different DNS servers owning and trading different parts of the map. They update their parts of the map on a regular basis, but in between updates they use the stored versions of the map (their DNS caches) to send users querying that system to their destinations and give the stored versions of their part of the map to other DNS servers as guides to their neighborhood.

With the system set up as it is, a single point of failure—the compromise of even one DNS server—can allow an attacker to poison the cache and mislead all users querying that DNS server. And some of these DNS servers, for example, those of Internet service providers, serve and can potentially mislead millions of users.

DNS Cache Poisoning

DNS cache poisoning lets online criminals make a legitimate domain name redirect not to the IP address that domain name is supposed to be affiliated with, but to an IP address of their choice. That means they can control where Web users go, sending them to malicious websites even if these users never clicked on a malicious link and instead carefully typed in legitimate website URLs.

This makes cache poisoning perfect for hosting malware or for making phishing sites even more successful. Most "regular" phishing websites don't use legitimate URLs, but URLs that look very similar to the real URL; for example, a website in which the letter "l" in the

domain name is replaced with the number "1"—making it hard for the visitor to detect that they are not actually visiting Mylegitimatebanksite.com, but instead My1egitimatebanksite.com.

Getting visitors to these fake sites usually requires using some kind of social engineering technique. But when criminals poison DNS caches, they don't need to use this subterfuge or send out spam linking to the not-quite-legitimate URLs. Instead, they use cached DNS records stored on DNS servers to control where Web users who correctly type in or click on a *legitimate* URL go. They essentially hijack all of the Web users who type in that URL (not just the smaller percentage that clicks on a link in an email or on another site), so that instead of ending up at the legitimate destination they typed in, the users are redirected to a malicious site.

For instance, typing in the legitimate URL Mylegitimatebanksite.com would not lead to that legitimate site, but could instead directly send users to a site that tries to download malware onto their computers, or one that looks similar to the bank's website but sends any information or passwords visitors type in straight to online criminals.

In mid-2008, major headlines were generated about a way of exploiting vulnerabilities in many vendors' DNS server software that could make it easier to poison DNS caches. Although DNS cache poisoning is not new, security researcher Dan Kaminsky identified a potentially more reliable and effective means of doing so.

For more information on DNS best practices, network protection, and attack identification, visit www.cisco.com/web/about/security/intelligence/dns-bcp.html.

TCP Stack Table Implementation Vulnerability

Recently, a security researcher disclosed that both known and unknown weaknesses in the TCP stack table implementations of many products could be exploited using an exploit called Sockstress. Detailed research has not yet been released, but initial findings suggest that affected products could include most operating systems, routers, intrusion prevention systems (IPS), and firewall devices, since they all handle TCP traffic with stacks that could be affected.

The researcher is known to be working with vendors and organizations to assist in creating fixes for the affected TCP stacks. Depending on the time required to develop fixes, full information may not be released until sometime in 2009, when this vulnerability will undoubtedly receive additional attention.

Networking Equipment Vulnerabilities

Although many IT departments spend significant effort patching and upgrading desktop systems, applications, and data center equipment, upgrading networking equipment sometimes gets short shrift. This can be because if the network is working well, it doesn't seem like a good idea to interfere and cause network downtime—and upgrading networking equipment can be complex.

However, not implementing regular upgrades to networking equipment can be dangerous. The amount of research into vulnerabilities in networking equipment and operating systems increased in 2008, including for Cisco products. And if exploits do start showing up in the wild, the consequences of attacks on corporate networking equipment could be severe. Unscheduled downtime is one potentially painful consequence. Or worse, sophisticated attackers could leave the network running smoothly, and focus on compromising and gaining access to sensitive data residing all over the network.

Virtualization Vulnerabilities

Corporate environments are widely embracing virtualization. Whether virtual or remote workers, virtual data centers, or network virtualization, all offer benefits in the areas of cost-effectiveness and flexibility. Data center and network virtualization as well as "virtual client" products may also enhance ease of administration and security.

However, some of these virtualization products are still relatively immature, and have not been rigorously tested for security in live environments. This led to 103 vulnerabilities being exposed in virtual software products between January and November 2008. In that same time frame, major virtualization vendor VMWare issued 18 security advisories for its products in 2008, compared to seven advisories for all of 2007.

> "As virtualization technology gains in popularity, it may bring with it new risks."
>
> —Don Simard, Commercial Solutions Director, U.S. National Security Agency in *InfoWorld*, March 13, 2008

"The more complex the threats become, the more you have to do the basics and groundwork *really* well. Staying aware and on top of new vulnerabilities and ensuring that patches and software updates are rapidly implemented is crucial."

—Jeff Shipley,
Cisco Intelligence Collection Manager

The increasing use of virtualization technologies in corporate environments is likely to make them attractive targets for additional attacks and exploits in the coming year.

Encryption Vulnerabilities

The growing number of employees working from remote locations, the increased risk of data loss through error or malice, and the urgent need to protect important information make encryption a key security tool. Organizations are depending on encryption to secure email communications, shared data repositories, and devices such as laptops, CD-ROMs, flash drives, and other memory devices that include sensitive data.

However, several encryption technologies have shown vulnerabilities. And weaknesses in encryption can cause a false sense of security, with users and network administrators thinking they are protected from certain threats when, in fact, they are not.

In one high-profile example, certain versions of the open source operating systems Debian and Ubuntu contain an OpenSSL vulnerability that could lead to pseudo-random values being generated—and that could be easily predicted. Using these values could also generate weak encryption keys and certificates or passwords, which would then be vulnerable to brute-force attacks. At the end of August 2008, it became clear that online criminals were using stolen SSH keys to attack servers running Linux, and installing a malicious rootkit on them. There is speculation that the OpenSSL vulnerability in Debian and Ubuntu may have played a role in these attacks.

With many organizations using Linux-based servers—which this exploit laid open to control by online criminals—to run important parts of their networks, this was an extremely serious concern to many IT departments.

One encryption system known to be weak remains in widespread use: WEP, which is used for Wi-Fi networks. WEP was broken years ago, attack and exploit tools are widely available, and hacking into WEP-encrypted Wi-Fi networks is easy. Yet many individuals and organizations continue to use WEP, which leaves them vulnerable to criminal activity.

Organizations that process credit card information, such as merchants and service providers, will soon be required (by the 2008 update to the Payment Card Industry Data Security Standard) to upgrade from WEP to the stronger WPA encryption for their wireless networks. But the myriad organizations that provide free Wi-Fi access are not required to make this switch, leaving the security of their networks porous. Many home users of Wi-Fi access points also leave their networks vulnerable to snooping and exploitation.

Operating System Vulnerabilities

Although vulnerabilities that affected all major versions of the Microsoft Windows OS and the Linux kernel showed up in 2008, overall, the number of OS vulnerabilities discovered declined compared to previous years. Most of these vulnerabilities require user interaction; very few are exploitable by unauthenticated remote attackers if the victim does not open a file or otherwise perform a required action.

Widespread acknowledgement of the importance of patching and regularly updating operating systems—and making patching easier—have significantly contributed to the decline in OS vulnerabilities. Microsoft's efforts in this area have been quite successful. So although OS vulnerabilities are still being reported, their decline indicates that attackers are increasingly looking to other classes of vulnerabilities to compromise systems and user information.

Vulnerabilities in Databases and Office Productivity Applications

The use of vulnerabilities in office productivity applications to conduct both targeted and widespread attacks continued in 2008. High-profile malicious code attacks involved products such as the Microsoft Office suite, Microsoft Jet Database Engine, Adobe Acrobat, and Ichitaro word-processing software from Japanese office productivity tools vendor JustSystems.

Interaction from the victim—for example, opening an attached document or malicious database file—is typically required for criminals to exploit these vulnerabilities and take control of targeted computers. Once attackers have control of the user's system, they could bypass certain perimeter defenses on a corporate network and launch additional attacks.

Files associated with these types of applications are well-suited for targeted attacks by knowledgeable attackers using social engineering techniques. For instance, an attacker might send a malicious spreadsheet labeled "Profit and loss statement for shipping department" to people in an organization's accounting group. The attacker could spoof the origin of the document by using easily found information from a corporate website, such as the names and email or physical addresses of executives. This is especially effective as spreadsheets and other office productivity files are commonly used in organizations for legitimate business. That means that users often trust them, and they're rarely blocked at the network perimeter.

Mobile Device Vulnerabilities

The BlackBerry, an essential part of modern workplace productivity, suffered from a vulnerability this year that could compromise corporate networks. Research In Motion (RIM), the makers of the BlackBerry, disclosed that the way BlackBerrys open PDF attachments could leave corporate networks vulnerable to being compromised.

Other smart phones are vulnerable as well. Weaknesses in installer applications have allowed Trojans to be installed on certain phones. And the Web browsers that some mobile phones use may make it easier for users to fall victim to phishing campaigns. For example, a mobile phone's Web browser may be configured so that the address bar doesn't show all of a long URL. With phishing sites, the first part of the URL often looks legitimate, but the latter part may give clues (an "off" top-level domain, or strings of numbers) of being a phishing site. Or the mobile phone's input method may make the process of manually entering URLs into the address bar arduous, so that users are more often tempted to "just click" on a possibly malicious link.

As with Web 2.0 technologies, some smart phones offer an open application development environment, which means that downloading a new application for the phone carries the risk that it might be malware. Or, if it wasn't developed using secure coding practices or thoroughly tested before release, it might merely be easily exploitable.

Geopolitical and Political Conflicts

Spam, malware, and botnets are being used to a greater extent as weapons in geopolitical and political conflicts, as in Estonia in 2007 and Georgia in 2008. It is estimated that this trend will continue in the years to come.

In the 2007 "Estonian Cyberwar" (said to have been a revenge attack in response to the Estonian government's removal of a statue of a Russian soldier from a prominent location in the capital), Estonian government, banking, and media websites were attacked and shut down using botnet-based DDoS attacks. Speculation continues about whether these online attacks were spontaneous, or occurred with Russian state backing.

In July 2008, in the weeks leading up to and during the Russian-Georgian conflict, Georgian government websites were defaced or shut down, as was the website of the National Bank of Georgia. According to reports in the *International Herald Tribune*, attacks were hosted out of servers in the U.S. as well as Russia, attesting to the flexibility of "cyber-warfare." Botnets affiliated with the Russian Business Network, a group of online criminals with ties to the Russian government, were used in the attack.

The Burmese junta has also used online methods against those protesting its regime. During the 2007 political protests in Burma, the junta shut down all Internet access for the country. (Burma has only one ISP, owning satellite phones is forbidden, and computers in Internet cafes log user activities by automatically taking a screenshot every five minutes.) This attempt to stop protesters from sending out digital photos and reports of the political protest was largely unsuccessful, so on the anniversary of the protests in September 2008, the junta reportedly used DDoS attacks to shut down dissident websites.

In many of these cases, it is and will remain very difficult to prove state backing of DDoS attacks against enemy websites. However, from a security perspective, being aware that geopolitical conflicts are more likely to include an Internet component—whether it is state-sponsored, or actions from individual hackers—can help organizations prepare for the chance that DDoS attacks may be used against a country's government, financial, media, or vital infrastructure websites.

In an interesting political twist, the 2008 U.S. election also saw DDoS attacks against the websites of certain political campaigns, such as that on a website urging votes and soliciting donations to counter a high-profile proposition banning gay marriage in the state of California. Using a DDoS attack, proponents of the proposition were temporarily able to deny visitors access to the opposition's website and impede their ability to donate money to its campaign during a fundraising drive.

Awareness that botnet activity is likely to increase during geopolitical and political conflicts may also be helpful in creating a proactive security strategy. And the apparent weakness of many state-run networks is important to address. If security professionals at these organizations remain alert to the fact that their networks and websites may become targets during conflicts, they may be able to strengthen their networks earlier and more thoroughly. For example, they could proactively monitor online discussions of techniques that may be used against them, allowing them to counter attacks with patches and workarounds.

> "You could fund an entire cyber-warfare campaign for the cost of replacing a tank tread, so you would be foolish not to."
>
> —Bill Woodcock, *Packet Clearing House* in *The New York Times*, August 13, 2008

From Conflicts to CyberCommands

For many years now, what could be termed low-level cyber-warfare has existed between semi-organized hacker groups with political, religious, and other motivations—for instance, between Israel and Palestine, China and Taiwan, India and Pakistan, and others. A recent change is the addition of overt state sponsorship and military backing for Internet-based warfare.

The escalation of cyber-warfare from semi-organized individuals or groups to state-sponsored activities brings a new level of resources, capabilities, skills, and organization to this arena. The governments of several countries, including the U.S. and China, have set about establishing "cyber-command" organizations. These organizations are tasked with protecting their respective countries from online warfare and with creating offensive cyber-warfare capabilities.

Even though more countries are pursuing this, there is an ongoing debate (often outside of military circles) about whether or when an offensive cyber-warfare capability is warranted or a sound decision. That is the experience of many network administrators has shown that trying to go on the offensive against Internet attackers seldom proved to be a sound, responsible, or fruitful decision.

Cyber-warfare has not been well-defined except as an extension of existing electronic warfare; interception and exploitation of communications would certainly be included under this concept. For example, in mid-2008, unclassified White House emails were exfiltrated, according to FBI sources. Origins of the attacks were traced back to servers in Russia and China, although the existence of state backing is difficult to prove. Security firms linked to the campaigns speculated publicly that foreign entities may be pursuing a "grains of sand" approach, in which large amounts of less-well-protected data is being carefully sifted for nuggets of important information.

In this context, it is interesting to note that governments around the world are implementing many privacy and wiretapping laws, or granting immunity to the telecommunications firms that enable wiretapping. Recent examples include a proposed U.K. law that would allow the government to collect data on all electronic communications. Another U.K. proposal would require user registration for all mobile phones, allowing the government to create a central database of all U.K. mobile users. Notwithstanding significant popular opposition to these proposals, this indicates an ongoing commitment to more closely monitoring communications that may have security implications. In many countries, average citizens will not be affected by this monitoring, unless there are security implications, such as international phone calls to countries or individuals of concern to state authorities.

Countering Internet Security Threats

Apart from working to minimize vulnerabilities and fighting back against current Internet security threats on a case-by-case basis, several broader initiatives are also being used in the battle for online security.

DNSSEC

Industry and governments are working hard to mitigate DNS vulnerabilities—the hot issue of summer 2008. Implementing Domain Name System Security Extensions (DNSSEC) is widely seen as crucial to ongoing Internet security, in that DNSSEC will provide integrity of DNS information to protect against spoofing and cache poisoning exploits.

Although most experts agree that deploying DNSSEC is crucial, adoption faces several challenges, such as implementation complexities and disagreements over who should own the top-level root keys. The top-level country code domains of Sweden, Bulgaria, Puerto Rico, and Brazil already use DNSSEC. And U.S. officials recently announced that DNSSEC would be implemented for the .gov domain by January 2009, and for all .gov subdomains by December 2009, which should further spur worldwide adoption.

Security vendors and researchers are collaborating more closely on the disclosure of vulnerabilities, so that patches and workarounds can be created before the exploitable information is widely available. Security vendors are also working both together and separately to make it easier to report and discover current security incidents, and to assess threats accurately. Government initiatives designed to enhance security are being implemented in several countries. And law enforcement is working to send online criminals to jail.

Industry and Government Initiatives

In two separate incidents, hosting providers for online criminals were shut down (InterCage in September 2008 and McColo in November 2008), thanks to efforts by security researchers or organizations, law enforcement, or ICANN. In both cases, the amount of spam sent out worldwide decreased noticeably for several days, until the hosting providers' clients found other providers. Although the long-term impact was limited, this was a positive step: Industry and law enforcement organizations were able to identify and collect evidence showing the malicious activity, and more importantly, positive action was taken by higher-level service providers to InterCage and McColo and organizations like ICANN.

There are other recent examples of law enforcement and courts working to stop or prosecute online criminal activity.

- In July 2008, Seattle "spam king" Robert Soloway was sentenced to 47 months in prison. Notorious for marketing spamming services that used botnets to send billions (or by his own account, trillions) of spam emails, often with spoofed headers that made it appear as though they came from Hotmail or MSN accounts, Soloway finally pleaded guilty to mail and email fraud.
- British hacker Gary McKinnon may be extradited and tried in the United States on charges of hacking into NASA as well as U.S. Pentagon, Army, Navy, and Air Force computers. McKinnon claimed he never harmed the computers, but was looking for evidence of alien technology.
- A U.S. District Court, acting on information collected by the Federal Trade Commission (FTC), shut down and froze the assets of a major international spam network known as HerbalKing. HerbalKing sent out billions of spam messages to market potentially unsafe versions of prescription drugs. The FTC received more than three million complaints about messages related to this operation. The court froze the spam network's assets and issued a temporary injunction that prohibits the defendants from sending spam and making false product claims. New Zealand authorities, working with the FTC, also took legal action against the spammers, and the U.S, government is planning to pursue criminal charges.

On the industry and government collaboration front, new organizations such as the Industry Consortium for the Advancement of Security on the Internet (www.icasi.org) are addressing multi-vendor global security threats and creating a forum for industry collaboration and innovation around security.

And industry standards continue to be updated to reflect changes in technology and security. The Payment Card Industry Data Security Standard (PCI DSS), for example, was updated in 2008 to mandate more secure wireless encryption technologies.

Meanwhile, National Computer Emergency Response Teams (CERTs) continue to play valuable roles in assessing threats and vulnerabilities, providing information on them, and coordinating vendor response, as do other government and industry associations.

In the area of identity theft, the U.S. government's 2008 Identity Theft Task Force Report indicated that in 2007, 2470 criminals were charged with identity theft-related crimes, while 1943 were actually convicted. The high rate of conviction for those prosecuted, combined with compliance requirements and more organizations following best practices around safeguarding personal information, is helping to reduce the likelihood of identity theft.

Yet criminals can still make large profits from identity theft-related crimes while the probability of prosecution is currently low. (To ensure sufficient prosecution of such crimes, the report recommended that the government review its civil monetary penalty programs.)

More thoroughly tackling identity-theft-related crimes will require a comprehensive approach toward ensuring greater individual awareness and additional security measures by businesses, as well as prosecution and international cooperation. To make further progress, increasing the reporting of such crimes to and cooperating with law enforcement will be especially important.

Enabling Technologies

Security vendors are actively working to make security simpler, which helps to enhance the implementation of and adherence to security tools and policies.

For example, vendors have been disclosing threats and releasing patches more quickly. And to help with crucial user education efforts, many vendors have been making it easier for end users to find information about security risks and threats and to assess their potential negative effects.

For many vendors and users, making security simpler with technology means creating security solutions that:

- Make it easy to establish and adapt security policies
- Automate security tasks (such as encrypting sensitive data or deploying patches)
- Offer protection within, as well as at the edges of, the ever-expanding network
- Closely monitor and assess threats in real time
- Protect from threats along multiple vectors
- Integrate with other security tools
- Empower workers to safely use new collaboration and productivity tools

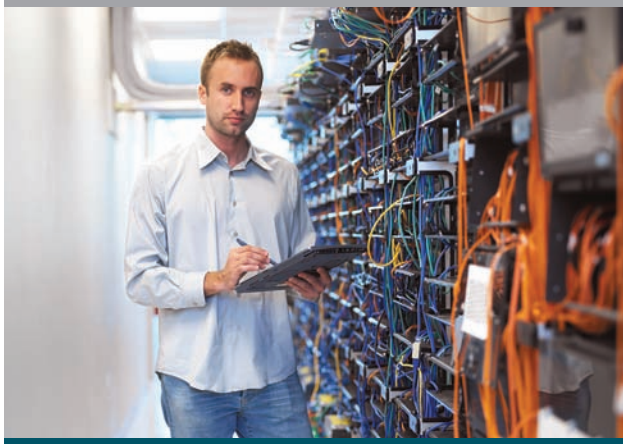
Making Security Easier to Find

A useful industry standard was created to make it simple to report security incidents and discover information about current security issues. This involved having companies create a standardized high-level "security" page on their websites, with a location that would be easy for visitors to remember. So, a user wanting to see the latest information about a known vulnerability that affects products from a company known as Example would just need to type "www.example.com/security" into a browser. Although some companies have implemented this standard, many are still lagging.

Standardized Security Page
cisco.com/security
microsoft.com/security
adobe.com/security
yahoo.com/security
facebook.com/security

Not Yet
apple.com
secondlife.com
google.com
mcafee.com
myspace.com

Conclusions and Key Recommendations



2008 marked both an expansion and evolution of the online security threat landscape. In some cases, online criminals reaped rewards of tens or hundreds of millions of dollars. This potential for profit will continue to drive nefarious innovation and specialization in the year ahead.

Threats that combine one or more online elements—the Web, spam, malware, and botnets—continue to grow in number and sophistication. For greater effectiveness, criminals are more and more often targeting specific individuals or groups and exploiting legitimate websites and other trusted entities and systems. They are launching increasingly hard-to-detect threats that can dupe even savvy, cautious users. And they use social engineering techniques and take advantage of current events to make their online schemes appear highly credible or appealing to their victims.

Meanwhile, the malware that is spread through online threats is constantly being redesigned to be smarter and more surreptitious than ever before—and it has an enormous growth rate. Botnets, the core of criminal activity on the Internet, continue to spread malware, send out millions of spam emails, host malicious websites, and attack legitimate ones. To counter these threats, organizations should include active anti-malware and botnet prevention components in their security strategies.

Online criminals are exploiting both old and new weaknesses in technologies and systems to create botnet armies. Known high-impact vulnerabilities are going unpatched. At the same time, increasing use of mobile devices and remote working, Web 2.0 tools, virtualization, and new forms of collaboration are all expanding the security perimeter and making the edges of the network more permeable. This poses a significant challenge when organizations try to shore up their defenses, and underscores the need for adoption of advanced security policies and technologies.

Data loss continues to be a challenge that can have grave, costly effects on organizations and individuals. Creating strong security policies can help, but these policies must be implemented and enforced throughout the organization. Regarding data loss, many organizations now assume that company equipment with sensitive information is likely to go missing at some point. As a result, they are also increasingly using tools and technology—including virtual private networks, content filtering at the gateway, authentication technologies, access controls, encryption, and data removal and truncation—to keep sensitive information from being accessed or used by unauthorized persons.

Insider threats are another issue that requires awareness and vigilance. In a troubled global economy, more of these attacks can be expected.

On the upside, expect to see more news stories in 2009 related to how authorities are combating offenders and spammers. By offering specialized, complex services, modern offenders are becoming more established, and tracking and catching them may become easier. However, even as security vendors and authorities collaborate to bring online criminals to justice, this does little to diminish the number of attacks.

Putting IT on the Front Lines

According to Cisco's August 2008 InsightExpress report, *The Challenge of Data Leakage*, approximately 50 percent of business workers worldwide mix business and personal use on their computers. For most companies, the blending of business and personal IT use is inevitable, but it makes defining and enforcing acceptable use policies that much more challenging.

In fact, a recent study by Cisco of the common failures of enterprise security policies revealed gaps between IT's perceptions of why policies are violated, and employees' true motivations. Most employees surveyed said they broke security policies because the policies either did not align with the realities of their jobs, or they needed to access applications not included in the policy, or both. Yet most IT professionals thought apathy and lack of awareness were the typical reasons for employees' security policy violations.

Many companies are struggling to define acceptable use policies that enhance security, but are not so inflexible that they stifle collaboration and the art of getting business done in today's highly competitive, Web-enabled world.

IT personnel can help with this, and should be at the forefront of combating security risks. According to the *2008 Global Information Security Workforce Study* from Frost & Sullivan, qualified and experienced personnel are the key to stopping security threats. They can work directly with management and employees to create and implement relevant and user-friendly policies that are practiced throughout all levels of the organization, starting in the boardroom.

But, if IT is to be more involved and effective at helping to ensure security across the enterprise, organizations must invest more in their IT departments. Ensuring that IT departments can access adequate resources and the most knowledgeable and experienced professionals—particularly, security specialists —is key.

It is also important to change the perception of the IT department's security policies from "forbidding" to "empowering." For example, when IT personnel recognize that employees will download the tools they want regardless of IT policies, they can offer realistic solutions to the problem, such as providing vetted versions of downloadable tools and creating secure pathways to content on work-related Web destinations.

When employees do inevitably make a mistake or inadvertently download something that compromises security, they should be encouraged to be open about it with IT so the issue can be addressed quickly. If the incident is the result of simple human error, without malicious intent, organizations should take a stance of demonstrating appreciation to the employee for helping to swiftly identify and combat the threat. This will encourage users not to feel fearful about informing the IT department about risks.

Employees can play a vital role in safeguarding their own online identity and understanding the risks that go hand-in-hand with their use of technology. Ongoing user education around security policies and technologies and online threats can help. An important benefit of companies educating and training their workforce about security risks and threats: It can ultimately lead to better technology practices in the employees' personal lives, thereby helping to keep online criminals at bay on two fronts.

Key Recommendations Checklist

- ✓ Stay focused.
- ✓ Stop users from inadvertently downloading malware onto the network.
- ✓ Patch known vulnerabilities.
- ✓ Prevent data loss.
- ✓ Take insider threats seriously.
- ✓ Remember the network.
- ✓ Think beyond compliance.
- ✓ Make security simpler.

Key Recommendations

Stay focused. One essential thing for organizations to keep in mind about security is that when they try to protect *everything*, nothing will be protected. Instead, organizations should focus most of their time, energy, and resources on what is strategically, financially, and competitively most important to safeguard.

Stop users from inadvertently downloading malware onto the network. To ensure that users cannot visit—or download the compromised parts of—webpages that contain malware, use several malware scanning technologies; proactive, real-time, reputation-based filtering solutions; and rule- and application-based firewalls and intrusion detection and prevention software at the network gateway.

Individual users can also significantly reduce their chances of falling victim to malware downloads. Keeping browsers fully updated and patched, using security features and settings, and remaining aware of existing and emerging threats is crucial, as is never clicking on a link received in email—even email from apparently trustworthy sources. Instead, users should always manually type in a trusted URL, bookmark it, and revisit it by using the bookmark rather than by clicking on links provided by others.

Patch known vulnerabilities. To be effective in today's landscape of evolving threats, security organizations must be aware of new trends. However, many current and emerging threats take advantage of *known vulnerabilities*, so organizations should not become wholly distracted by emerging threats. Spending time, energy, and resources on addressing and patching existing defects in their security armor remains essential.

Around 80 percent of common attacks take advantage of 20 percent of high-impact vulnerabilities. These high-value vulnerabilities are often very basic, and continue to be unpatched in certain environments. Staying up-to-date on these high-value vulnerabilities (and securing them) will, in most cases, lead to a good "80/20" solution.

Prevent data loss. Strong security policies are essential for protecting an organization from the negative effects of data loss. But these policies must be enforced to be effective, and users must be made aware of them.

Recommendations for reducing the risks associated with data loss include:

- Deploy methods (preferably automated) to maintain the confidentiality of information on mobile devices such as laptops, thumb drives, and PDAs through methods such as access controls, encryption, remote data removal, data association, redaction, truncation, or other methods that effectively render data unusable.
- Classify data and put stronger controls on what data people can access.
- Define which data should be protected, so that the focus is on keeping the most critical information the most secure.
- Educate users about what information should not be stored on a laptop or other mobile device, and what to do if such equipment is stolen.
- Actively monitor email and Web traffic to ensure that sensitive information is not being shared inappropriately.

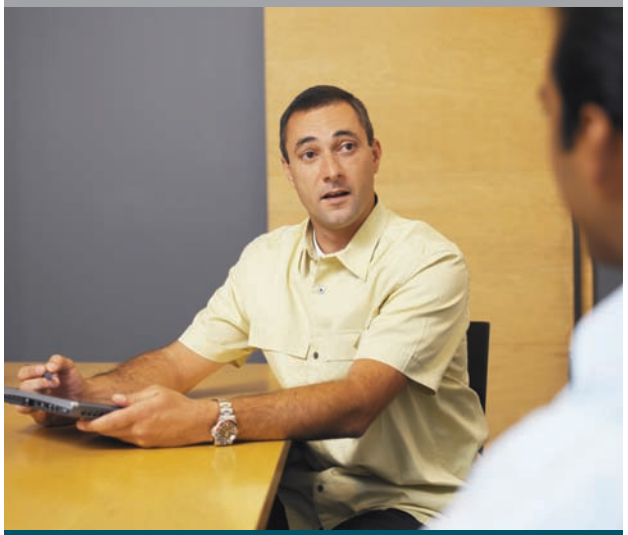
Take insider threats seriously. Be vigilant by continually logging, auditing, and monitoring traffic patterns, systems, and databases. Set policies that prevent employees from engaging in unauthorized activities. Businesses should ensure that their information security teams coordinate with physical security teams and HR departments to implement effective policies for revoking access of terminated or transferred employees. Always conduct thorough background checks during the hiring process.

Remember the network. Enterprise security is not just about headline-grabbing malware threats and data breaches. Despite being a security blind spot for many organizations, network devices are at risk, too. Many organizations use an "if it's not broken, don't fix it" approach to their networks—especially in a cost-conscious, down economy. While most organizations should upgrade their networks at least once a year, the optimal upgrade frequency depends on size, complexity, security requirements, resource constraints, and other considerations.

Think beyond compliance. Organizations should not let compliance be a security placebo. By focusing almost exclusively on compliance, and aligning their procedures to meet those requirements, organizations can lose sight of the current, rapidly evolving risk and threat environment. In addition to reviewing compliance levels, organizations should conduct regular top-down gap analyses to augment existing procedures and proactively meet current and emerging threats.

Make security simpler. Above all, make security tools and solutions easier to implement and use, and make security policies easier to follow.

- Layer integrated sets of security technologies, rather than depending on patchwork and point solutions.
- Ensure that security solutions and departments effectively share data.
- Set security policies that protect all important assets, and make their implementation automated and straightforward.
- Teach IT departments and employees to work together to enable safe access to productivity-enhancing tools and content—both within and outside corporate networks.
- Keep existing network and security hardware and software patched and updated in ways that don't impede productivity.
- Work continuously on user education and awareness of new threats, and encourage users to report possible or suspected gaps in security.



Top Trends to Expect in 2009

To help organizations develop their security strategies and plan their IT budgets for 2009, Cisco has identified the following key trends to watch for in the year ahead. These predictions are based on news and events from 2008, as well as related information and insight provided by Cisco's security and business operations worldwide.

Smaller, More Frequent, Targeted Attacks

More sophisticated attacks will occur in the year ahead. They will be deployed rapidly and designed for even more specific targets—individuals, groups, businesses, organizations, and governments. The current worldwide financial crisis is still playing out, natural disasters and manmade strife will continue to provide global news hooks, and a new U.S. president is taking office in 2009. Criminals will certainly keep refining how they take advantage of (and profit from) these types of news events.

Social engineering and phishing techniques have been profitable, so offenders can be expected to keep refining the delivery method for (and improving the success of) these attacks. There will be more "specialists"—criminals who deliver one or more key components essential to creating a complex and convincing attack. As they grow their expertise and reputation, these specialists will be sought out and hired by others looking to create their own high-impact attacks.

Cross-Protocol Attacks

Online criminals looking to improve their odds of success will increasingly rely on cross-protocol or "blended" approaches that combine email, Web-based threats, and intrusions. This type of attack, successful in recent years, will keep growing during 2009. Also expect to see more botnets that are capable of "multitasking"—for instance, sending spam, hosting malware, *and* launching a direct attack.

To defend against more robust multi-protocol attacks, organizations will need to implement security systems that can monitor all Internet traffic types and rapidly identify and stop new threats. Security solutions that focus on only one area (such as email, IPS or Web-based threats), or those that cannot effectively correlate data between areas, will not be enough to protect organizations from blended threats.

Reputation Hijacking

Hijacking reputations has proven attractive and effective for online criminals. When people trust a brand, they are likely to visit an associated site or open an email from that source without question. Many traditional or point security solutions depend on URL or IP filtering lists and don't have real-time insight into traffic patterns and suspicious behavior from every element on a webpage; these solutions are not equipped to recognize that a trusted website or email sender has gone bad.

In 2009, more online criminals will be actively hijacking reputations and will work on finding additional, more sophisticated ways to do so.

Mobility, Remote Working, and New Tools as Risk Factors

The trend of remote working and related use of Web-based tools, mobile devices, virtualization, "cloud computing," and similar technologies to enhance productivity—especially in an economic climate that demands leaner, more-cost effective and global staff—will continue in 2009.

This means that preventing loss of data—from outside attacks, insiders, or negligence around data storage devices such as laptops—will become more crucial than ever. But it will be a challenge for security personnel. The edge of the network is expanding rapidly, and the increasing number of devices and applications in use make the expanding network more porous, creating new inroads for threats.

Organizations of all types should implement thorough, sensible data loss prevention (DLP) policies and consider security solutions that automatically prevent sensitive data from leaving protected environments.

Every organization should also begin to take simple steps designed specifically to protect intellectual property—an increasingly precious asset in the modern economy.

A Holistic Approach to Security

Cisco's vision for security is enabling customers to collaborate with confidence. To do so, Cisco champions a holistic, proactive, layered approach to counter existing and emerging security threats.

Cisco Security Intelligence Operations is an advanced set of capabilities that provides threat detection, correlation, and mitigation to continuously enable the highest level of security for Cisco customers. Using a combination of a team of global research engineers, sophisticated security intelligence, and automated update systems, Cisco Security Intelligence Operations allows customers to securely collaborate and embrace new technologies.

With the increase in blended, cross-protocol, and cross-vendor vulnerability threats, the security industry has come to recognize that point defenses that protect from individual threats or protect individual products are no longer enough. Integrated security management, real-time reputation assessment and a layered, multi-point approach are the new watchwords.

Cisco Security Intelligence Operations will use tightly integrated data derived from multiple Cisco divisions and devices to continuously assess and correlate Internet threats and vulnerabilities. Sources of this data include:

- **Cisco's worldwide Threat Operations Centers**, at which over 400 researchers track new trends and threats.
- **Cisco Security Remote Management Services**, a 24-hour-a-day, 7-day-a-week team of highly-certified, experienced security and network professionals who provide operational support for security incident monitoring, fault and performance incident management, problem resolution, security infrastructure tuning, and secure network access control support.
- **The SenderBase Network**, which monitors 30 percent of all Web and email traffic worldwide and handles 30 billion queries every day. To assess the real-time reputation and trustworthiness of every active Web server on the Internet, the SenderBase Network tracks more than 150 different network-level parameters.
- **Cisco Security IntelliShield Alert Manager**, a customizable alert service that provides up-to-the-minute, actionable intelligence, in-depth vulnerability analysis, and highly-reliable threat validation.
- **Cisco Intrusion Prevention Systems**, which identify, classify, and stop known and unknown threats, including worms, network viruses, application threats, system intrusion attempts, and application misuse.
- **Real-time network traffic telemetry data** provided by Cisco network devices, which will be implemented in Cisco products starting in 2009.
- **A variety of other Cisco functions,** including Cisco Security Research and Operations, Cisco Security Incident Response, the Corporate Security Programs Office, and Global Policy and Government Affairs.

With Cisco, organizations can save time researching threats and vulnerabilities, and focus more on taking a proactive approach to security.

As Internet threats continue to evolve, Cisco Security Intelligence Operations will enhance Cisco's ability to identify global threat activities and trends, and provide expert analysis and services to help protect users from these threats. Cisco is committed to providing complete security solutions that are integrated, timely, comprehensive, and effective—enabling holistic security for organizations worldwide.

For More Information

Cisco Security Center
www.cisco.com/security

SenderBase
www.senderbase.org

Cisco Security Solutions
www.cisco.com/go/securitysolutions
www.cisco.com/go/ros

Cisco Security Products
www.cisco.com/go/security
www.cisco.com/go/intellishield
www.cisco.com/go/ips
www.ironport.com

Cisco Corporate Security Programs Organization
www.cisco.com/go/cspo

Report available for download at

www.cisco.com/go/securityreport

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at **www.cisco.com/go/offices**.

C02-512160-00 12/08