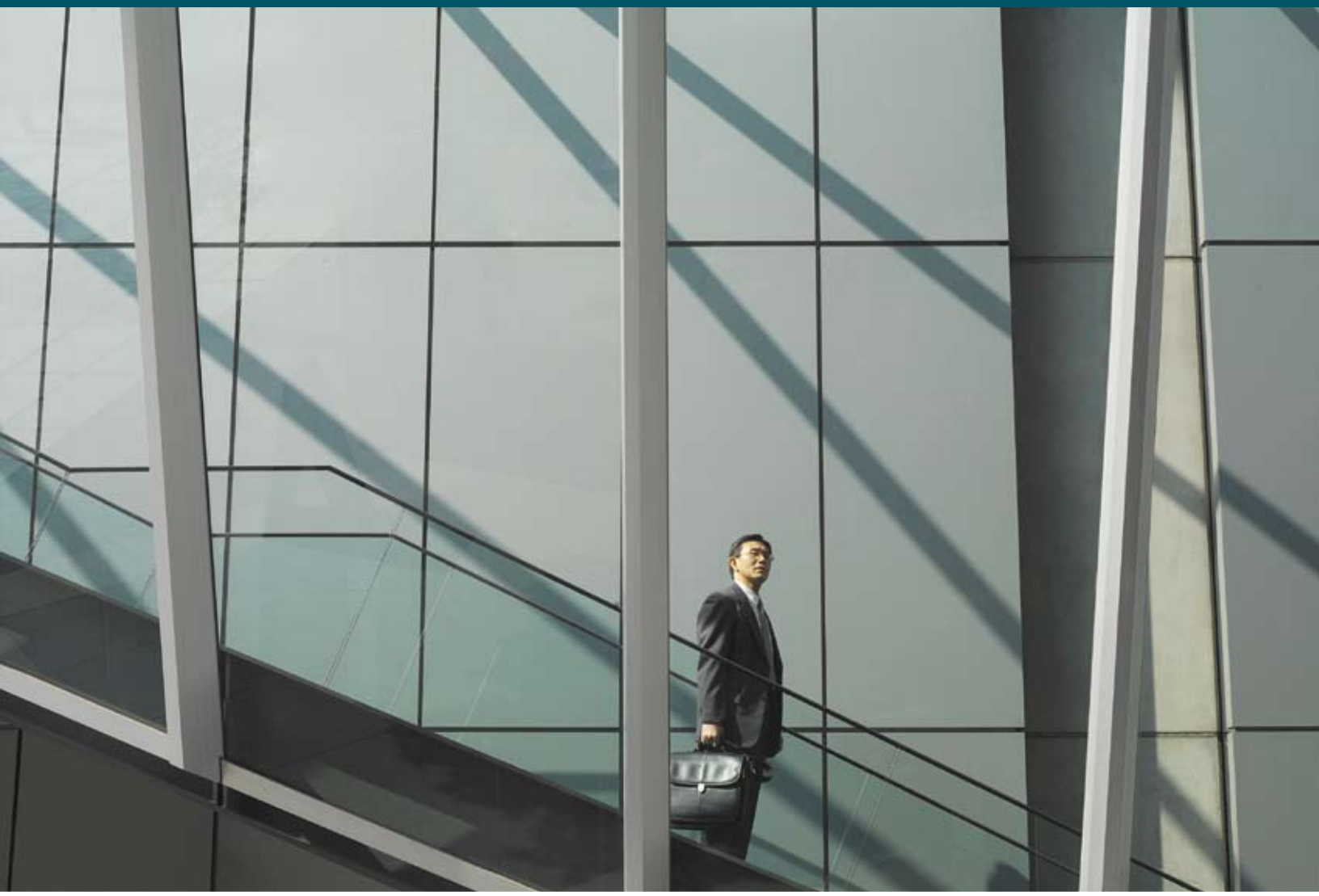
Cisco 2007 Annual Security Report



Contents

Executive Summary

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 September 2007, and provides a snapshot of the state of security for that period. The report provides recommendations from Cisco security experts and predictions of how identified trends will continue to unfold in 2008.

Security trends and recommendations are organized into seven major risk categories:

- Vulnerability
- Physical
- Legal
- Trust
- Identity
- Human
- Geopolitical

The report also provides a high-level perspective on the issues currently shaping the security space, as well as insights into how security professionals and businesses can expect the industry to change over the next several years.

Understanding Security in an Insecure World

> "Uncertainty is the only certainty there is, and knowing how to live with insecurity is the only security."
>
> —John Allen Paulos, best-selling author[1]

The 21st century is characterized by a growing interconnectedness between businesses, governments, and individuals. This unprecedented connectivity has led to enormous social and economic benefits, but has also introduced numerous new risks. As Internet and network technologies continue to automate more business processes and democratize access to information, people can work, communicate, and interact in ways that were inconceivable just a few years ago. A fully connected world also means, however, that a determined individual with an Internet connection can wreak havoc on individuals, governments, or even entire industries, and affect the lives of millions of people.

The year 2007 was characterized by unprecedented innovation and adaptability in the realm of security threats, as criminals once again demonstrated their ability to continually evolve attack strategies to keep ahead of even the most advanced human and technical defenses. Fortunately, 2007 also saw the continued growth of an overarching trend that is allowing organizations to combat threats more effectively than ever before: an increasingly mature understanding of the nature of the online criminal situation.

Earlier in the modern "Information Age," security analysis tended to look inward—focusing on operating systems, Internet browsers, and other software applications businesses used that made them vulnerable to attack. By 2007, however, most corporations based security policy on an acknowledgment that the real threat is not technology, but people—or more specifically, people with criminal intent. And more businesses recognized that, just as in the offline world, criminals will exploit any vulnerability they can find and monetize.

Another aspect of the evolving understanding of modern "cybercrime" in 2007 was a growing recognition that cybercrime is a crime, and that the main motivator in most crime is money. Whereas just a decade ago, information attacks were largely an issue of vandalism, today they are like any other crime. Today's information attacks are a profitable business enterprise and are often controlled by organized crime syndicates. Among other significant trends underscoring this reality, 2007 saw a growing number of sophisticated cybercrime business models, including the emergence of criminal enterprises built around selling tools and services for launching network attacks, rather than simply selling information gained from attacks.

At the same time, recognizing this type of crime as a for-profit venture has led to new approaches to thwart it. Rather than simply trying to block every possible attack, governments and businesses in 2007 increasingly focused on strategies (such as prosecuting spam purveyors and targeting monetary drivers of cybercrimes) that make attacks more difficult and less profitable.

Finally, in 2007, more and more businesses, governments, and law enforcement agencies recognized the truly global nature of cybercrime. That understanding has brought about recognition of the need for greater cooperation and collaboration between businesses, governments, and law enforcement agencies across all industries and continents to thwart criminals more effectively.

This report presents an overview of these trends and others, drawn from the significant amount of security information gathered throughout Cisco between January and September 2007. It is intended to provide a concise summary of the major security issues of the past year, as well as key security recommendations from Cisco experts and forward-looking analysis of what to expect in 2008 and beyond. Ideally, this report can provide an important tool to help organizations make better decisions about how they approach evolving security risks, and where they focus security resources and attention.

[1] A Mathematician Plays the Stock Market, Basic Books, 2003

Cisco Security Methodology

The information collected in this report is the result of extensive information gathering and comprehensive, collaborative effort across multiple Cisco global operations functions. Much of the intelligence compiled here was published throughout the year by the Cisco Security IntelliShield Alert Manager Service and through the IntelliShield Cyber Risk Reports. The Cisco Security IntelliShield Alert Manager Service's team of expert analysts compile the risk reports using a broad range of automated data-collection tools that continuously monitor human and electronic information sources from all regions of the world.

In addition to IntelliShield Alert Manager resources, Cisco security intelligence draws on the security expertise of contributors from across Cisco global operations, including:

- The Cisco Information Security (InfoSec) team, an internal team that is responsible for securing the global Cisco network
- The Cisco Product Security Incident Response Team (PSIRT), responsible for defending against Cisco product vulnerabilities
- The Cisco Applied Intelligence Engineering Team
- The Cisco Advanced Services Security Practice
- The Cisco Corporate Security Programs Organization
- Cisco security product development teams responsible for Cisco firewall, intrusion prevention, access control, and VPN solutions
- The managed security arm of Cisco Remote Management Services
- Analysts from IronPort (acquired by Cisco in January 2007), who continually track spam and malicious e-mail trends from around the globe
- The Cisco Global Policy and Government Affairs team

Experts from these and other areas meet weekly to discuss the latest security issues and trends, and to compile IntelliShield Alert Manager alerts. This broad range of security expertise, as well as the global scope of Cisco business operations, allows Cisco to gather up-to-the-minute security intelligence from an unprecedented number of sources and extend that knowledge to customers. From legal issues to geopolitical concerns to hands-on knowledge gleaned from network engineers responding to threats in the field in real time, Cisco is able to build an unparalleled community of security expertise and information.

Using This Report

This report encompasses information and trends collected between January and September 2007. Like IntelliShield Cyber Risk Reports, this report is organized into seven major risk categories:

- Vulnerability
- Physical
- Legal
- Trust
- Identity
- Human
- Geopolitical

Vulnerability

> "Better be *despised* for too anxious apprehensions, than *ruined* by too confident security."
>
> —Edmund Burke, 18th-century politician[2]

There was both good news and bad news for the vulnerability category in 2007: The biggest issues of the past—operating system (OS) and server OS vulnerabilities—decreased dramatically. After being subjected to so many attacks over the years, leading operating systems, particularly Microsoft Windows desktop and server platforms, have matured and become more robust. That's the good news. The bad news is that, given the improving security of operating systems, attackers are now looking for other vulnerabilities to exploit. They are finding plenty of vulnerabilities in applications that run on top of the OS or play an integral role in the functionality of the OS, such as Sun Microsystems' Java.

The total number of threat and vulnerability alerts published by Cisco Security IntelliShield Alert Manager Service between January and September actually declined in 2007 as compared with the same period during the previous year. However, new vulnerabilities in applications (including software such as the Microsoft Office suite, Adobe Acrobat, and others) rose 14 percent in 2007 from 2006. Software product vulnerabilities published by Cisco Security IntelliShield Alert Manager Service have increased by double-digit percentages each of the past several years, and that trend continued in 2007. Fortunately, Cisco identified a relatively small number of vulnerabilities that were actually exploited and attacked. Given the inherent difficulties in protecting the myriad applications that can exist in a business environment, however, many organizations' security teams had a difficult time keeping up.

Other major vulnerability trends in 2007 included a host of new, highly sophisticated malware attacks, the emergence of new tools to help attackers create more effective attacks, and new forms of spam designed to evade conventional filtering techniques.

Overall Threat and Vulnerability Alert Trends

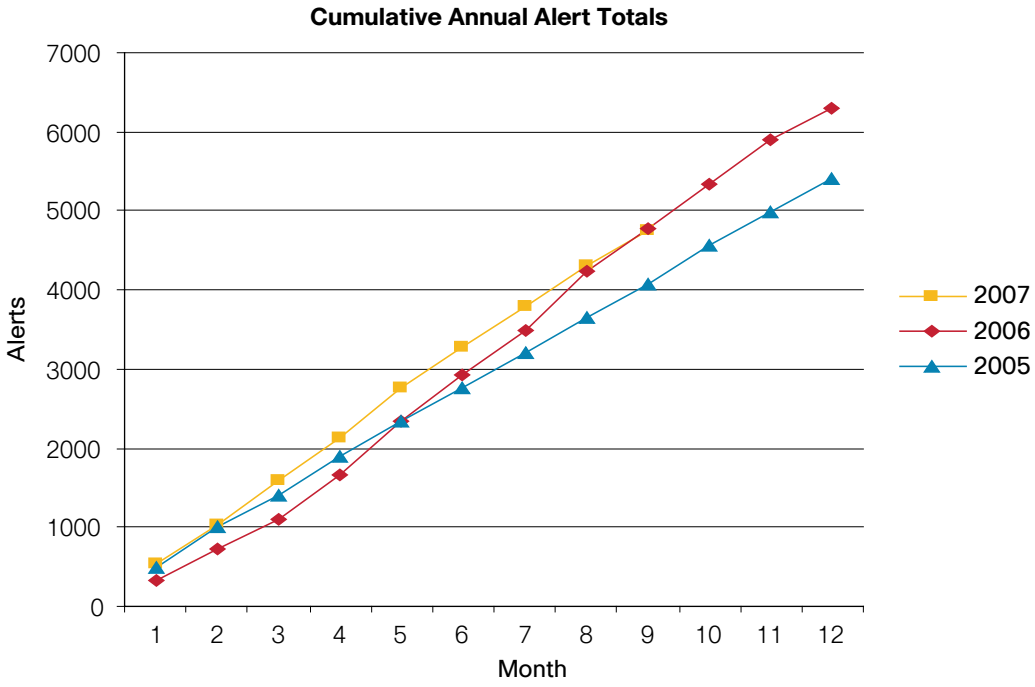
The number of threat and vulnerability alerts issued by Cisco Security IntelliShield Alert Manager Service declined during the period of January to September 2007 over the same period in 2006 (Figures 1 and 2). Early in the year, the number of alerts appeared to be following the same 12 to 16 percent increase that Cisco Security IntelliShield Alert Manager Service had seen in the three previous years. By April, however, the number of alerts had begun to flatten, and that trend continued for the remainder of the time period.

Figure 1. Total Threat and Vulnerability Alerts Published by Cisco Security IntelliShield Alert Manager Service

Year	Jan-Sep Total	Annual Total
2005	4078	5412
2006	4773	6301
2007	4760	–

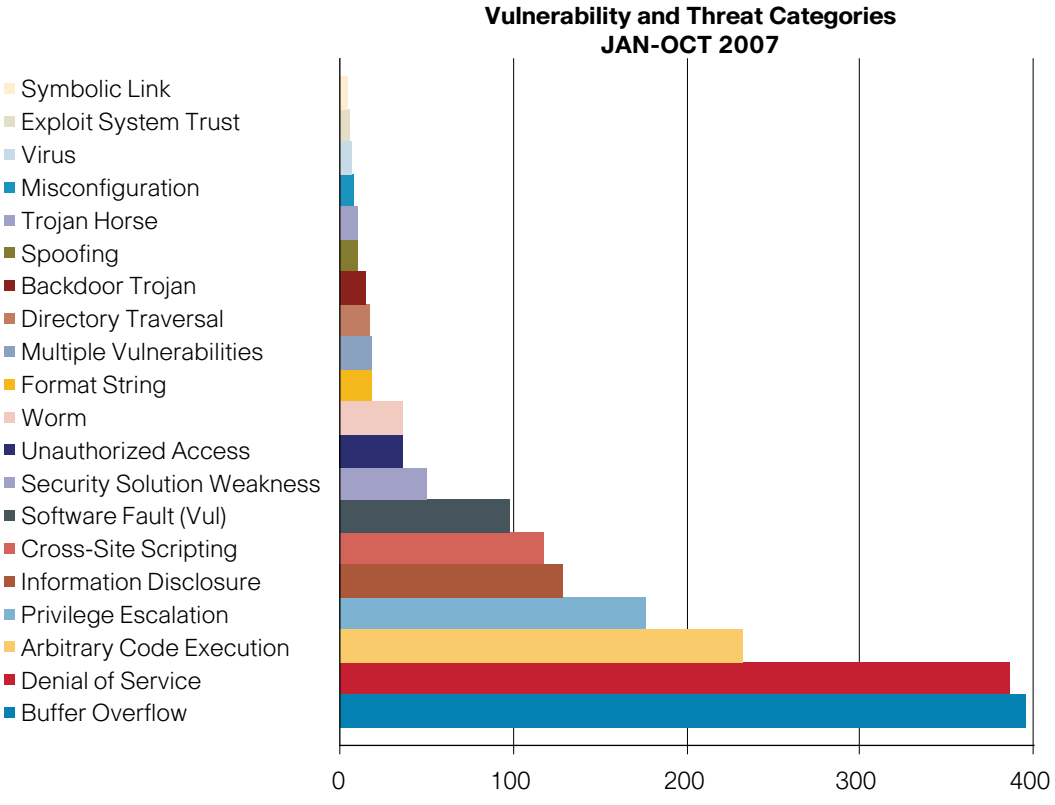
[2] The Works of the Right Honorable Edmund Burke, Little, Brown, and Company, 1877

Figure 2. Cumulative Cisco Annual IntelliShield Alert Manager Alerts



Cisco security analysts identified numerous threat and vulnerability issues in 2007, but Cisco Security IntelliShield Alert Manager Service issued the most alerts for Denial of Service (DoS), buffer overflow, and arbitrary code execution threats (Figure 3).

Figure 3. Top 20 Threats and Vulnerabilities, January through October 2007



Major shifts in reported threat and vulnerabilities as compared to the same time period in 2006 included a drop in new worms and Trojans, directory traversal attacks, exploited misconfigurations, and symbolic links; and an increase in software vulnerabilities and buffer overflow attacks (Figure 4).

Figure 4. Shifts in Threats and Vulnerabilities Reported

Threat Category	Alert Count	% Change from 2006
Arbitrary Code Execution	232	–24%
Backdoor Trojan	15	–72%
Buffer Overflow	395	23%
Directory Traversal	17	–52%
Misconfiguration	8	–57%
Software Fault (Vul)	98	53%
Symbolic Link	5	–64%
Worm	37	–28%

Cisco Security IntelliShield Alert Manager Service rates the urgency and severity of alerts using a scale from 1 to 5 that is based on the IntelliShield Alert Manager risk management formula. The overall urgency of reported threats (representing the level of activity of the threat) declined in 2007 compared to the same time period in 2006; however, the overall severity (representing the potential impact of a successfully exploited vulnerability) increased (Figures 5 and 6). Ultimately, these trends indicate that fewer active threats emerged in 2007, but those that were active could cause significantly more damage if successful.

Figure 5. Overall Urgency of Threats, January through September 2007

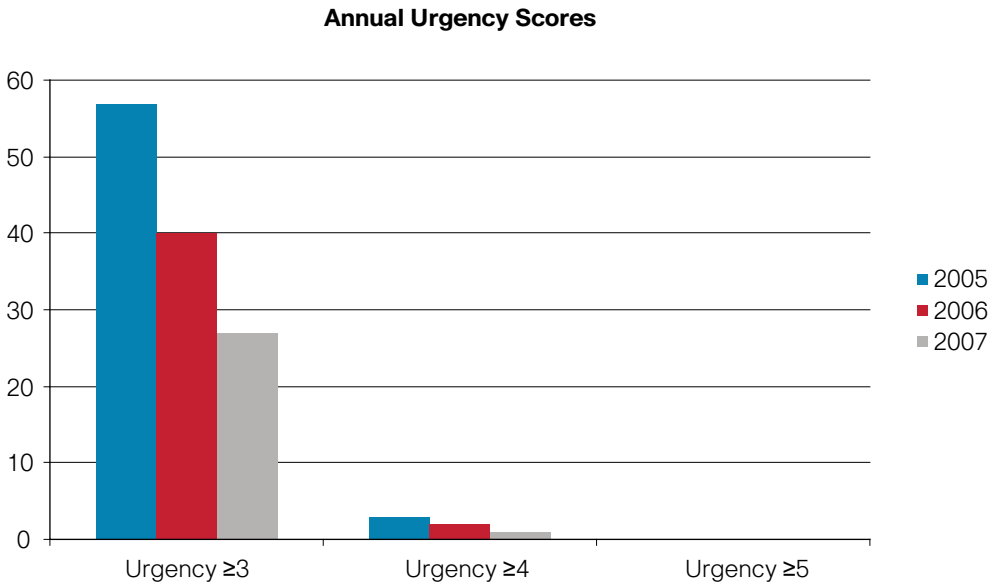
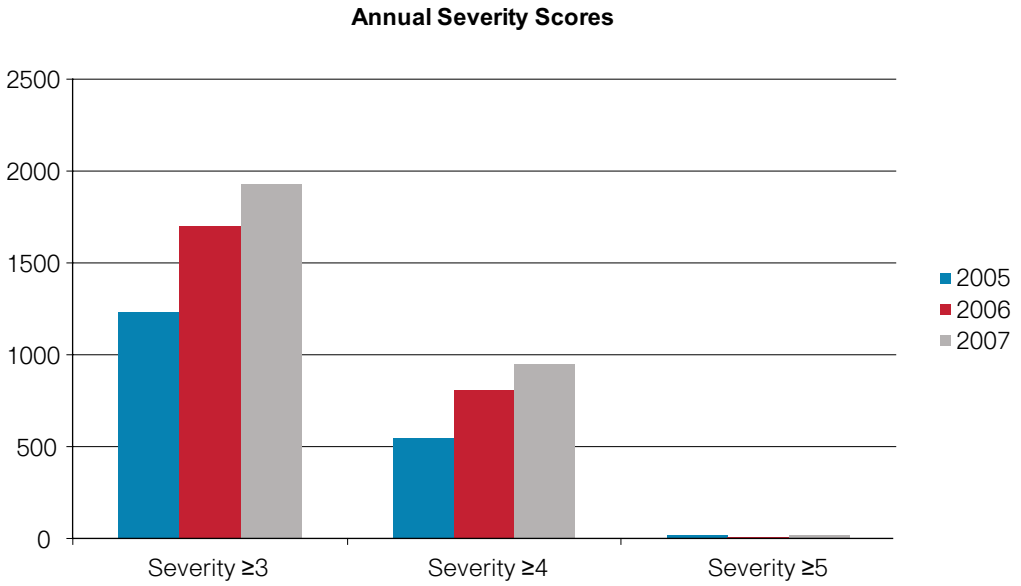


Figure 6. Overall Severity of Threats, January through September 2007



Web Application Attacks on the Rise

The number of e-commerce, customer relationship management (CRM), and other Web applications grew in 2007—and presented a significant number of new vulnerabilities. There are several reasons for this trend: As criminals and security researchers studied these applications for the first time, they discovered many vulnerabilities that were previously unidentified. In addition, most languages used to create Web applications had not previously had to stand up to the rigors of attackers continuously seeking exploits. These languages proved to have serious vulnerabilities. Finally, instead of choosing from a handful of operating systems, attackers in 2007 could consider hundreds of different Web applications, making the list of potential vulnerabilities exponentially longer. RealNetworks RealPlayer, Apple QuickTime, and Sun Java Web applications are just a few examples of applications with vulnerabilities that attackers sought to exploit.

Growing Exploitation of Productivity and Security Applications

The year 2007 also found attackers increasingly looking to business applications to launch attacks. Attackers used vulnerabilities in products such as the Microsoft Office Suite, the OpenOffice suite of applications, Adobe products, and Symantec antivirus software suites to conduct both targeted and widespread attacks. Since these types of applications are widely used in business settings, they presented attackers with an attractive alternative to OS exploits for ensnaring large numbers of systems.

For the most part, attacks designed to exploit these vulnerabilities relied on "social engineering"—enticing a user to interact with a malicious document in some manner, such as opening or loading a document. However, since the types of files used in such attacks often have legitimate business applications, they were generally allowed to pass through e-mail filtering techniques.

Major business application exploits in 2007 included:

- *Mdropper and PPDropper*—Trojans such as Mdropper and PPDropper successfully exploited previously unknown ("day-zero") vulnerabilities in Microsoft Word and PowerPoint applications.
- *Trojan.Pidief*—This Trojan, discovered in October 2007, exploits a known vulnerability in Adobe Acrobat.

- *Ginwui*—The Ginwui family of Trojans was updated multiple times in 2007 to produce additional variants designed to exploit more recent vulnerabilities as older ones were patched. Several high-profile vulnerabilities disclosed in 2007 were used in such attacks, including:
  - Microsoft Office Malformed String Arbitrary Code Execution Vulnerability
  - Adobe Reader Hosted PDF File Cross-Site Scripting Vulnerability
  - Microsoft Word Arbitrary Code Execution Issue
  - Microsoft Word Malformed Data Structure Arbitrary Code Execution Vulnerability
  - Microsoft Word Malformed Function Vulnerability
- *Rinbot*—Rinbot, also known as Nirbot, first appeared in February 2007. The worm appeared to target Symantec applications and propagate by exploiting known vulnerabilities, including the Symantec AntiVirus and Client buffer overflow vulnerability, as well as the Microsoft Windows DNS Server interface buffer overflow vulnerability. More than 20 variations of this worm have appeared since February 2007; however, the number of Rinbot variations has decreased as vendors have corrected the vulnerabilities.

Vulnerabilities Turned into Actual Attacks

While relatively few application vulnerabilities discovered in 2007 were actually exploited by malicious code, several significant attacks did circulate in the wild. Major vulnerabilities that were exploited included:

- Microsoft Windows ANI File Handling Arbitrary Code Execution Vulnerability
- Microsoft Windows Font Rasterizer Privilege Escalation Vulnerability
- Microsoft Windows DNS Server RPC Interface Buffer Overflow Vulnerability
- Apple QuickTime Movie and QTL File Handling Cross-Domain Scripting Vulnerability
- Cisco IOS® Software Voice Service Session Initiated Protocol Denial of Service Vulnerability
- Microsoft Windows VML Buffer Overflow Vulnerability
- Apple Mac OS X DiskManagement BOM File Handling Privilege Escalation Vulnerability
- Sun Solaris Telnet and Login Combination Unauthorized Access Vulnerability

Some of the highest-impact malware exploits of 2007 included:

- *Storm worm*—Of all malware attacks of the past year, the Storm worm (also commonly known as Peacomm, Nuwar, and Zhelatin) garnered the most media attention. In addition to the large number of systems the worm has infected, the attack is also significant as an example of a continually evolving, highly adaptable exploit, as well as its tendency to lay dormant for weeks or months, and then return in a new format. Storm arrived in users' inboxes as a ZIP attachment, a greeting card, a password-protected RAR attachment, a URL, and an MP3 attachment at various times during the past year. The primary goal of Storm may be to add infected systems to a malicious botnet. Once a system is part of the botnet, attackers can easily use the network to distribute spam or potentially launch a distributed denial of service (DDoS) attack. Reports indicate that portions of the Storm botnet are being sold to certain groups for spamming purposes. The bottom line is that the botnet is huge (potentially tens of millions of systems), the attack's authors are highly skilled at adapting to evade detection and prevention, and Storm continues to be successful. Cisco analysts expect to see even bigger attacks orchestrated from this botnet in the coming year.
- *Gozi*—Gozi, also known as Ursnif, received considerable media attention in 2007. The Trojan was created by Russian malware authors and targets primarily home computers, although it has compromised accounts at financial, retail, healthcare, and government organizations as well. As of October 2007, Gozi had compromised almost 5200 hosts and 10,000 user accounts.

- *Anicmoo*—Anicmoo exploited the Microsoft Windows ANI file handling arbitrary code execution vulnerability in large-scale attacks. Attackers delivered the Trojan as malicious HTML e-mail messages or hosted it on malicious Websites, allowing them to remotely execute arbitrary code on infected systems. Cisco observed variants of this code for multiple platforms, including Windows XP SP1 and SP2, and Windows Vista. Analysts reported that attackers could easily modify the worm to bypass current antivirus signatures.

Malware Attacks Continue to Evolve

Malware attacks became more sophisticated during 2007. In addition to continually adaptable exploits such as Storm, notable malware trends included:

- *Increasingly sophisticated strategies to steal account information*—The Infostealer.Banker Trojan demonstrated a creative new method of stealing confidential information. The Trojan monitors a targeted user's Internet browsing activity and waits until the user accesses login screens of certain online banking Websites. The Trojan then intercepts communication between the Website and the user's browser, causing the browser to display additional fields in the login form, which may include PINs, Social Security numbers, and other information not included in the legitimate form. The Trojan records a copy of all submitted data and sends it to an attacker-controlled, remote Website.
- *ARP-poisoning attack*—W32.Arpiframe, which performs a new, sophisticated attack, surfaced during 2007. The worm first performs an Address Resolution Protocol (ARP)-poisoning attack against hosts that reside on the same subnet as the infected system. This attack aids a "man-in-the-middle" attack, which allows the infected system to act as a proxy server for the local subnet. The worm can then modify all HTTP requests made by browsers of local systems. The attack places an infected iFrame in various Websites that may be accessed by users on an infected local network. The actual Websites are not compromised, but for all users accessing those sites through the infected network, the sites contain infected iFrames that downloaded malicious code onto the user machines.
- *Mobile device attacks*—A 2007 Informa Telecom media study claimed that more than 80 percent of mobile operator respondents suffered malware infections in 2006, and that the number of incidents was more than five times higher than the previous year.
- *XML Trojans*—Malicious code writers have recently begun to develop XML-controlled Trojans, and several examples were found in the wild in 2007. These Trojans exploit the trusting nature of XML to provide a control channel over port 80, allowing them to pass commands to infected hosts without triggering notifications on firewall and IPS/IDS devices.
- *Multiplatform worms*—Several multiplatform worms emerged in 2007, including Badbunny (which was distributed as an OpenOffice Draw file) and MSIL.Yakizake (which uses the .NET framework to propagate across Windows-, Solaris-, and Linux-based machines through the Mozilla Thunderbird e-mail application).
- *Instant messaging (IM) worms*—A growing number of IM-based malware attacks, including W32/Skipi.A, also known as the Skype worm, materialized in 2007. Generally, these attacks launch an IM window with a link referencing the malicious code, and transmit the message to all IM contacts on the infected machine.

Growing Market for Malware Development Tools and Services

One overarching trend that has dominated the world of malware for the past several years is the reality that cybercrime is no longer an issue of pranks and vandalism, but a hugely profitable criminal industry, increasingly dominated by organized crime. Three malware innovations in 2007 highlight this paradigm:

- *Emergence of subscription-based attack services*—A number of Websites appeared in 2007 offering viruses, Trojans, and other malicious code for sale. The business model of such

sites was based on customers installing the code on other Websites and receiving monthly payments based on the amount and quality of information collected from infected machines. Some of these services even offered ongoing service and support for their customers. The most significant innovation along these lines, however, was the creation of the 76service portal through service provider Russian Business Network (RBN). Built around the Gozi Trojan, 76service offers a highly functional Web portal through which subscribers can pay for access to user information on Gozi-infected systems. The portal includes streamlined controls to help subscribers easily manage groups of infected machines and quickly view and extract private information.

- *Growing availability of exploit toolkits*—Malicious code developers are creating more toolkits to install malware, allowing attackers to more easily create exploits for different threat scenarios. These tools are publicly available for sale and can be modified to accept new vulnerabilities. The most significant example of this trend in 2007 was MPACK, an exploit tool that compromised more than 10,000 Websites worldwide.
- *Increasing sales of phishing tools*—Multiple sites emerged in 2007 offering tools to automate phishing attacks and allow even low-skilled attackers to launch sophisticated attacks. Tools included Flash animations to duplicate legitimate Websites that evade most antiphishing defenses.

Document-Based Spam Makes a Big Impact

The biggest spam delivery innovation of late 2005 and 2006 was the emergence of image spam, but 2007 saw the rise of a new strategy: spreading spam within document attachments. By employing common office document files to deliver spam messages (usually "pump-and-dump" stock scams), spammers were able to elude traditional spam filtering techniques. The most significant examples of this type of spam outbreak in 2007 were:

- *PDF spam outbreak*—This outbreak used a PDF attachment designed to look like a legitimate investment newsletter. The use of a PDF—the first major instance of a PDF being used for spam—fooled many users and presented a difficult challenge for conventional spam filters. In a single 24-hour period, the outbreak generated approximately five billion messages, representing nine percent of total spam volume, and making it one of the largest outbreaks of 2007.
- *Excel spam outbreak*—Building on the success of PDF spam, spammers launched an outbreak in July using Microsoft Excel attachments. As with the PDF outbreak, the use of a legitimate business file hampered the ability of many organizations and conventional spam filters to block the messages. Within hours of the launch, the combined Excel and PDF spam outbreaks represented as much as 17 percent of total spam volume.

Number of Malicious Websites Grows Dramatically

The use of Websites to host malicious code exploded in 2007. Antivirus vendor Sophos reported in April that it was identifying 30,000 new malicious Websites per day. These malicious Websites—as well as many legitimate sites that were infected with malicious code—infected millions of users in 2007. Major compromises included the Websites for the Sydney Opera House, Dolphin Stadium (which hosted the Super Bowl in February 2007), and the official Website for the Syrian Embassy in London. Additionally, the Colorado Rockies Major League Baseball team Website crashed just as ticket sales began for the World Series, as a result of what the U.S. Federal Bureau of Investigation (FBI) believes may have been a coordinated DDoS attack.

Key Recommendations

- *Focus on defending against high-severity vulnerabilities.*
  New OS and application vulnerabilities are likely to be continually discovered, and organizations cannot fully and immediately protect themselves against all of them. Businesses should focus the bulk of their defense efforts on high-severity vulnerabilities that are being actively targeted for exploitation.
- *Closely monitor and log applications.*
  All organizations should have strong policies and procedures in place to continually monitor the behavior of all applications in the environment.
- *Be vigilant about patching.*
  Keep applications up to date with all patches and bug fixes to remove known vulnerabilities.
- *Educate users and continually reinforce education.*
  Since most malware attacks still rely on users to launch the code, organizations need to continually reinforce the importance of never clicking on an e-mail attachment, document, or URL from an unknown or untrustworthy source. Attachments or URLs that arrive unexpectedly, even from a trustworthy source, should be checked to ensure that they were intentionally delivered.
- *Redouble efforts to secure Web application code.*
  Security companies have created Web application tools to help developers better test their code and more easily discover vulnerabilities, but some developers still do not appropriately test their code. Organizations should be asking vendors more questions about security and letting vendors know that application security is a major concern.
- *Continually monitor security intelligence for attack trends.*
  With thousands of vulnerabilities already known and more being discovered every day, organizations cannot realistically protect against all of them. By monitoring attack trends and the types of vulnerabilities that are being exploited, businesses can make better decisions about where to devote security resources and attention.
- *Employ host-based IPS solutions whenever possible.*
  Organizations should strongly consider using host-based IPS solutions on all workstations and servers to help protect against unknown vulnerabilities and day-zero attacks.
- *Monitor Websites for infiltration by malicious code.*
  Since users are apt to trust well-known sites, organizations must continually guard against attackers seeking to use their Web presence to spread malicious code.
- *Continue employing proven methods to keep attacks out of corporate networks.*
  Organizations should restrict file formats that are commonly associated with malware, employ spam filtering to block malicious e-mails, and use firewalls to prevent or limit the impact of malware attacks. Businesses should be vigilant in following effective security practices, such as placing anti-ARP spoofing measures on all switches that service user-accessible subnets.

What to Expect in 2008

- *Malware attacks exploiting application vulnerabilities will continue to grow.*
  Cisco security analysts expect the problem of application vulnerability exploits to become more significant during the next several years. IT security personnel can expect an ongoing battle on this front for the foreseeable future.
- *Expect more sophisticated attacks from professional attackers.*
  The number of organizations targeted by professional attackers is likely to grow. While much of the current professional cybercrime activity targets home users, organizations will likely see more infected systems attempting to access protected networks.
- *More malware may execute in system memory, not on hard drives.*
  Malware attacking rootkits that executed entirely in system memory emerged during 2007. As average RAM size continues to increase in the coming year, these strategies will likely grow in popularity.
- *More malware will target smartphones.*
  The huge increase in the use of multipurpose smartphones such as the Apple iPhone during the past year means that there are more mobile devices with fully functional operating systems in use than ever before. Future mobile malware will take advantage of the richer capabilities of these operating systems. Expect future mobile malware attacks to propagate via mobile e-mail, SMS, WiFi, and instant messaging applications.
- *More malware will target portable media and gaming devices.*
  As more users take advantage of growing storage capacity in iPods and other flash media to store sensitive business information, expect attackers to target these devices.
- *Expect more multiplatform attacks.*
  As malware development increasingly becomes a for-profit business enterprise, attackers will be looking to generate more value from their efforts by striving to hit more systems with a single attack project. Expect to see more attacks designed to target a variety of systems and platforms.

Physical

> "The superior man, when resting in safety, does not forget that danger may come. When in a state of security, he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered, and his States and all their clans are preserved."
>
> —Confucius, Chinese philosopher and founder of Confucianism

Physical security issues in 2007 centered around six major areas:

- Convergence of physical and information security systems
- Natural disasters
- Communications infrastructure damage
- Security control issues
- Disaster recovery system failures
- Lack of effective emergency response alert systems
- Emergence of blended physical and online attacks

Physical and Information Security Systems Converging

In 2007, more businesses implemented physical security solutions that run on IP networks, including IP-based video surveillance and electronic access control (i.e., badge and door lock) systems. By migrating these systems to the IP network, many businesses improved the scalability, resiliency, and intelligence of physical security solutions. (For example, some businesses integrated badge reader systems with network security systems, helping to eliminate issues such as building intruders accessing the network by blocking ports to employee PCs when the employee leaves the building.) This trend also allowed such organizations to manage more of their security from a single, open platform, instead of multiple, proprietary infrastructures.

At the same time, the convergence of physical and IP security creates new vulnerabilities. If critical physical security services (such as video feeds from IP surveillance cameras) are traversing the network, those services must be protected. For example, in 2007 the security penetration testing organization ProCheckUp demonstrated that one common Axis IP surveillance camera could be hijacked, granting the attacker access to the network.

Natural Disasters Affecting More Businesses, in More Ways

There were major earthquakes, tsunamis, and other natural disasters in China, Peru, Indonesia, and Japan during 2007. These natural disasters caused enormous damage to physical infrastructure and property. Major events included:

- Multiple earthquakes in Indonesia and China
- An 8.0-magnitude earthquake in Peru that buried the South Pan-American Highway in landslides
- Torrential rains and flooding in South Asia
- Multiple earthquakes in Japan, including one that resulted in the shutdown of the Kashiwazaki-Kariwa nuclear plant north of Tokyo
- Massive storms in the United States and Europe that downed power lines and caused major disruptions in air travel

With more technology-based industries operating in South Asia, South America, and other regions prone to natural disasters, even localized events are increasingly having an impact on more businesses and industries.

Communications Infrastructure Damage Becomes Growing Concern

Several instances of damage to fiber-optic cabling and other critical communications infrastructure occurred in 2007, some due to accident and some to intentional harm. Instances included the intentional cutting of an Internet-backbone cable serving millions of users in the Cleveland, Ohio area; the accidental removal of 43 km of fiber-optic cable in Vietnam by a salvage team; and damage to Internet2 communication cables in Boston, Massachusetts from accidental fire.

The market price of copper also increased worldwide in 2007. Not surprisingly, this trend led to more instances of copper theft for scrap metal, as well as damage to cabling infrastructure that thieves believed to contain copper. Even legitimate salvage teams accidentally damaged active cabling as the number of salvage teams operating grew.

Security Controls Prove Vulnerable

Control technologies and policies continue to evolve and improve, but 2007 demonstrated that no control is foolproof. Major control-related issues of 2007 included:

- *Security gaps at Sky Harbor Airport in Phoenix, Arizona*—The discovery of major security issues at Sky Harbor Airport in July provided an excellent example of how inconsistent enforcement of controls can undermine an entire security effort. The airport employed a variety of strong control mechanisms, but during evening hours when the airport did not host flights, many of the controls were not enforced. Security checkpoints were left vacant by Transportation Security Administration (TSA) agents, X-rays and metal detectors were inactive, carry-on luggage was not searched, and individuals were able to pass through checkpoints easily. The result was an environment that was extremely vulnerable—despite the fact that it was well secured for a large portion of each day. And, since security at every U.S. airport implicitly trusts security at every other U.S. airport, the breach at Sky Harbor also put airports across the country at risk.
- *Ongoing evidence that radio frequency identification (RFID) security can be undermined*—2007 saw growing adoption of RFID tags into security systems. While RFID vendors continued working to make RFID tags more difficult to copy, security analysts demonstrated at several conferences that RFID—even more sophisticated "smart RFID" chips, such as the ones being used in passports—need to be properly secured to reduce vulnerability to exploit.
- *Physical locks easily compromised*—Prominent security specialist Mar Weber Tobias warned IT security professionals in March that attackers can compromise 95 percent of common pin tumbler locks within seconds, and that most IT managers overlook this threat when securing IT systems.

Disaster Recovery Systems Far from Foolproof

While all data centers claim view-preserving availability as a critical function, many do not actually test recovery systems but instead assume they are functional. In a 2007 Forrester Research survey of 200 data centers, just 33 percent of respondents described operations as "very prepared," while 23 percent did not test disaster recovery procedures, and only 40 percent tested plans more than once a year.

One of 2007's most significant examples of flawed disaster recovery was the power failure and subsequent major service interruption at the 365 Main Datacenter (which hosts a number of major Web-based businesses) in San Francisco in July. 365 Main had a detailed disaster recovery plan and had backup generators in place to respond to a power outage. The unique characteristics of the outage, however—power fluctuating on and off throughout the day, causing the backup generators to repeatedly power up and power down, eventually draining their batteries—caused the backup system to fail.

Emergency Response Procedures May Still Lack Effective Alert Systems

An often-overlooked security consideration for responding to disasters, terrorist events, and large-scale acts of violence came to the fore in 2007: the need for effective systems to alert people in the vicinity of the incident. The Virginia Tech shootings in April, for example, demonstrated that, while emergency responders have made major strides over the past several years in improving communications to deal with violent emergencies, significant challenges still remain. In the Virginia Tech event, campus police, local police, and emergency responders all coordinated their response effectively. Unfortunately, while the critical information reached all appropriate responders, the university was not able to effectively alert the large population of students and employees on campus. The university sent out an e-mail, but since the attack occurred in the early morning hours, many students and instructors had not yet checked their mail when they arrived on campus and were unaware of the danger.

Blended Attacks Targeting Both Physical and IT Domains

In 2007, criminals demonstrated their evolving ingenuity by employing blended attacks to obtain sensitive information and evade detection. The most significant example of this trend was a string of attacks on Stop & Shop supermarkets in Rhode Island. Attackers broke into and vandalized supermarkets, leading police to believe the events were largely petty crimes. But during the break-ins, attackers tampered with the stores' card readers to collect credit card information.

Key Recommendations

- *Strive for a holistic operational approach to security.*
  Attackers will locate the simplest method to accomplish their goal, regardless of an organization's internal structure for managing security. Businesses should pursue consolidation and collaboration between physical and information security groups.
- *Address any potential vulnerabilities in physical security solutions running on the IP network.*
  If a company deploys a physical security device, such as an IP surveillance camera, over the network, administrators need to ensure that these endpoints are just as well protected as any other network endpoint. Collaboration among physical security teams (who typically control video surveillance) and IT security teams (who have the experience to properly safeguard IP networks) is essential.
- *Expect to deal with major disasters, especially in regions prone to them.*
  Businesses operating in regions with a history of natural disasters—and businesses that depend on such organizations—need to continually test, update, and train on disaster recovery and business continuance plans.
- *Contingency plans must address employees as well as infrastructure.*
  Secondary damage from natural disasters, such as roads becoming impassable, can create significant lingering problems. Disaster recovery plans should include considerations for how employees can communicate and continue operating the business, even if they are not able to work onsite for an extended period of time.
- *Protect essential cable infrastructure.*
  Organizations should redouble their efforts to secure all access points to critical infrastructure, ensure that cabling is well labeled, and educate local populations that may interact with the infrastructure. Organizations should not rely on a single physical connection for critical sites.
- *Have effective alert systems in place.*
  In planning response for violent events, organizations should ensure that communication systems and procedures address a broad spectrum of people who might be involved. Systems such as SMS messaging or basic loudspeakers can play a vital role in alerting employees and others in the vicinity.
- *Don't be overconfident in security controls and disaster recovery systems.*
  Having appropriate controls and procedures in place does not mean that an organization is secure. Security controls must be continually monitored and tested, and environments must be continually analyzed to identify potential new issues. Disaster recovery systems should be tested, not just against basic loss-of-service, but against unexpected scenarios and multiple points of failure.
- *Enforce security policies and controls uniformly.*
  Even when an organization has the most advanced security controls money can buy, if it does not apply controls consistently, 24 hours a day, the environment is not secure.
- *"Defense in depth" is as necessary for physical controls as for network security.*
  Organizations should use deterrent controls, such as signage and perimeter fencing, and detective controls, such as cameras and security guards, to reduce access to physical locks. Administrative controls such as sign-in/sign-out policies and escorts for visitors can also act as deterrents. Organizations should also ensure that locks are appropriate to their use and properly installed. Placing a strong lock on a weak door or locking a door between adjoining spaces with a shared ceiling crawlspace is not effective security.

What to Expect in 2008

- *Natural disasters will affect more organizations.*
  As global businesses become more interdependent and technology-based industries become more prevalent in countries prone to natural disasters, the impact of these natural disasters will continue to become more widespread.
- *Cable infrastructure will present an increasingly attractive target.*
  As more complex technologies are deployed in the public sector (and as the price of copper continues to rise), infrastructure will become a more attractive target for theft and attacks.
- *Blended physical and electronic attacks will increase.*
  Attacks against organizations are increasingly likely to be blended threats, occurring within multiple domains. Attackers will use physical means to access electronic information, and electronic information to compromise physical assets.

Legal

> "The search for static security—in the law and elsewhere—is misguided. The fact is security can only be achieved through constant change, adapting old ideas that have outlived their usefulness to current facts."
>
> —William O. Douglas, associate justice of the United States Supreme Court, 1939–1975

One of the most encouraging trends of 2007 was an increasing recognition by private organizations, law enforcement agencies, and governments that stopping Internet crime requires mature laws, extensive cooperation (especially across national boundaries), and improvements in regulatory compliance.

"Cybercriminals" Increasingly Prosecuted and Convicted

There was an unprecedented number of successful convictions of attackers and illegal spammers in 2007, demonstrating that lawmakers and law-enforcement agencies have become more technology-savvy in the ways they track, arrest, and prosecute cybercriminals. Examples include:

- Trial of the creators of the Fujacks/Panda family of viruses in China
- Arrest of creator of variants of the Cabir virus in Spain
- Conviction of spammers Jeffrey Goodin, Jeffrey A. Kilbrine, and James R. Schaffer under the U.S. CAN-SPAM Act of 2003
- Arrest of Robert Alan Soloway, one of the top e-mail spammers in the world
- Sentencing of former San Diego Council of Community Clinics (CCC) network engineer John Paul Oson to 10 years in federal prison for hacking into the CCC network

Growing Recognition of Need for Greater Cooperation

Major cybercrime activity in 2007 demonstrated unequivocally that Internet-based crime has become a truly global affair. Fortunately, there was increasing cooperation in 2007 among international businesses, governments, and law enforcement in trend monitoring, data collection, and criminal prosecutions. Examples include:

- Efforts by MySpace to monitor sex offenders and disclose sex offender account information to attorney generals from several U.S. states
- Likely extradition of cyber-attacker Gary McKinnon from Britain to the United States, representing the first case of an individual being extradited to the United States to face computer-hacking charges
- Arrest of identity thief "Lord Kaisersose" through successful cooperation between the U.S. Secret Service and the French National Police
- Arrest of an Alberta, Canada resident for illegal credit card data sharing thanks to cooperation between the U.S. Secret Service and the Calgary Police Service

Security Regulations More Consistently Enforced

While many information security regulations have been passed during the last several years, particularly in the United States and Europe, many of these regulations began to mature and be enforced in 2007. The Sarbanes-Oxley Act, for example, was intended to strengthen accountability and protection of financial information, but many organizations viewed the act as providing little actual improvement despite the enormous costs of complying with it. In 2007, regulatory groups responsible for enforcing Sarbanes-Oxley streamlined and clarified many compliance requirements. The first audits of U.S. healthcare organizations for compliance with the Health Insurance Portability and Accountability Act (HIPAA) also occurred in 2007.

Business Crimes Exposed

Several companies were caught or accused of engaging in illegal activities and corporate espionage in 2007. Prominent examples include complaints filed by Oracle that a subsidiary of SAP engaged in unauthorized downloads of Oracle data and distributed Oracle software, while reporters and former employees sued Hewlett Packard for illegally acquiring their phone records.

Key Recommendations

- *Private industry and government agencies must continue forging closer relationships to fight cybercrime.*
  As cybercrime evolves as a global enterprise, successful prosecutions require greater cooperation in monitoring, data collection, and coordination of activities across departments, national boundaries, and languages.
- *Organizations should continue targeting the monetary drivers of cybercrimes.*
  Complying with information security policies and pursuing convictions of cybercriminals makes it more time-consuming, expensive, and dangerous for attackers to engage in illicit activities—even if only a small percentage are actually brought to justice.
- *Ensuring flexibility is key.*
  Private- and public-sector organizations should recognize that maintaining flexibility and protecting the ability to innovate in security responses is crucial for achieving security. Laws and regulations should not mandate particular security technologies, methodologies, or procedures, as any requirement will quickly become obsolete as threats and defenses continue to evolve in the real world. Innovation and flexibility are key to security.

What to Expect in 2008

- *Fewer legitimate businesses will engage in spam- and adware-based advertising.*
  As more arrests and prosecutions involving adware and spam-based advertising become successful, vendors of these services will have a harder time finding clients.
- *Regulatory compliance auditing will become more prevalent.*
  Businesses will need to continue to devote resources to become and remain compliant. But, with improved clarification and definition of the requirements, businesses will be able to better focus their efforts and will be rewarded with actual improvements in their security postures.
- *Business crimes will continue as competition becomes fiercer.*
  Organizations should take strong precautionary measures to protect assets from corporate espionage, and to educate employees on corporate policies against such actions.

Trust

> "*Distrust* and caution are the parents of security."
>
> —Benjamin Franklin[3]

Overconfidence in trusted controls, systems, and individuals remains one of the biggest risks organizations face.

Insider Threats Continue to Present Serious Problems

Organizations have long recognized that attacks or breaches launched by trusted insiders can cause enormous damage. However, many organizations still did not have effective defenses against insider attacks in 2007 and suffered as a result. Examples include:

- A network administrator for a subsidiary of Fidelity selling the personal and financial information of 8.5 million customers to a data broker
- A terminated employee of the California Independent System Operators who was able to access the data center and put the Western United States power grid at risk
- A Social Security Administration employee caught selling identity information
- A United Kingdom policeman sentenced for stealing data from a police database
- A former employee of the Boeing Company accused of stealing more than 300,000 files, estimated to be worth between US$5 and $15 billion

Trusted Systems Prove Vulnerable

A wide range of security breaches and crimes in 2007 succeeded because of overconfidence in trusted information and security systems. Examples include:

- Demonstrated compromises of distributed antivirus and software backup agents that would allow attackers to spread malicious code to all systems hosting the agent
- Demonstrated vulnerabilities in Xen virtual machines that could allow attackers to infect multiple clients
- Legally mandated disclosure of separate pieces of voting data in Ohio, which, when combined, could reveal individual voting records
- Crippling of thousands of PCs in China after Symantec antivirus software mistakenly identified critical .dll files as malware
- Report by the Ponemon Institute that 40 percent of companies do not use security monitoring software on databases, and that more than 50 percent do not have proper security protocols in place to protect against insider database attacks

[3] Poor Richard's Almanack for 1850–52, J. Doggett Jr., 1849

Key Recommendations

- *Implement robust defenses against insider attacks.*
  Organizations need to continually log, audit, and monitor traffic patterns, systems, databases, and employees. Businesses should also ensure that information security teams coordinate with physical security teams to implement effective policies for revoking access of terminated employees.
- *Improve employee vetting and partner due diligence*
  Businesses need to increase scrutiny of employees, as well as inspection and authorization of partners, to protect their information assets.
- *Don't be overconfident in security controls, applications, or individuals.*
  Organizations should continually test security policies and controls. Security administrators should not trust what appears to be happening, but should research and test using actual data to ensure they have a clear picture of the environment. Systems and key personnel should operate with checks and balances whenever possible.
- *Compartmentalize to avoid pervasive failures.*
  Organizations that rely heavily on distributed antivirus or backup agents and virtualized environments face significant risk that a single breach could rapidly infect large numbers of systems or clients.

What to Expect in 2008

- *Trust issues will continue to present a significant problem.*
  Organizations will continue to be vulnerable to insider attacks, as well as to outsiders who discover poorly configured devices or new methods of exploiting the trust that users put into current systems.
- *Protecting the business' reputation will become increasingly important.*
  More businesses will direct additional efforts and resources toward monitoring external-facing Websites, applications, and databases to protect against malicious code and safeguard their reputations.
- *Businesses will need to devote more resources to mitigate internal threats.*
  More businesses will realign their security activities to increase internal controls and monitoring to limit employee and partner access and authorization.

Identity

> "If you *reveal your secrets* to the wind, you should not blame the wind for revealing them to the trees."
>
> —Kahlil Gibran, early 20th-century artist, poet, and writer

Identity theft continued to rise in 2007. A Gartner report released in March 2007 indicated that incidents have increased by more than 50 percent since 2003, affecting close to 15 million potential victims. While the goal of identity theft is always the same, the techniques criminals used in 2007 varied widely, with physical theft, social engineering, keylogging, and other techniques all playing a part in these crimes.

In addition to the significant damage that identity theft can cause for victims, these crimes can result in enormous losses for businesses. The IT Policy Compliance Group published a study in March reporting that organizations with publicly acknowledged thefts lose about 8 percent of revenue, and on average, incur US$100 per compromised customer record to notify customers and restore stolen data.

Major Thefts Snare Millions of Identities

The most publicized identity issue of 2007 centered around ongoing repercussions from the theft of more than 45 million customer credit card records from a TJX Companies apparel store in Florida in 2006. The identity theft highlighted several important issues, including:

- *The global nature of identity crimes*—Data stolen involved records from the United States, Puerto Rico, the United Kingdom, and Ireland, and was used to make illegal purchases in the United States, Hong Kong, and Sweden. Arrests resulted from cooperation between the U.S. Department of Justice, the Canadian Mounted Police, and other agencies.
- *Poor security controls*—The theft occurred due to weak encryption on the store's wireless network. A lack of monitoring and auditing allowed the thieves to gain extensive access to customer databases and to continue collecting data for an extended period of time.
- *Flawed Payment Card Industry (PCI) data standards*—Three quarters of the stolen credit cards had expired at the time of the theft, but the store was required to retain this outdated information anyway to comply with PCI standards.
- *Lack of prompt and full disclosure*—TJX Companies compounded the problem by failing to disclose the full extent of the breach in a timely manner, leading to multiple lawsuits and a significant hit to the company's reputation.

Other major identity incidents in 2007 included:

- Theft of a hard drive containing data for 1.3 million doctors and nearly 200,000 patients from the U.S. Department of Veterans Affairs (VA)
- Loss of a VA portable hard drive containing information on 535,000 people
- Loss of a hard drive from the U.S. Transportation Security Administration containing records of approximately 100,000 employees
- Discovery of a security breach at Kingston Technology Company through which billing information for 27,000 clients was stolen over the course of two years
- Loss of a CD containing unencrypted information on thousands of Alcatel-Lucent employees

Academic Networks Present Attractive Targets

Colleges and universities also proved vulnerable to security breaches and identity theft in 2007. Incidents included:

- Infiltration of a server used by the University of Colorado Boulder, revealing personal records of 45,000 individuals
- Theft of 14,000 records from an Ohio State University computer, and theft of two notebook PCs containing information on 3500 students from the home of a university professor
- Compromise of University of California San Francisco server, putting personal and financial information of 46,000 people at risk

Key Recommendations

- *Continually re-evaluate controls on identity information.*
  Organizations should constantly evaluate data access controls, storage, and transit systems to ensure that proper protections and inspection points are in place. They should also continually monitor databases and networks to ensure that breaches are identified as quickly as possible. In general, businesses should consider looking for ways to reduce the amount of personal information they collect. Finally, they should strive to develop enforceable policies governing data storage on portable devices.
- *Implement rational policies for retaining personal information.*
  Organizations need effective policies for expiring unneeded customer information to reduce their exposure in the event of a security breach. They should be pushing for revised PCI standards that address this problem.
- *Safeguard information through physical and information security.*
  Attackers will increasingly seek to exploit any perceived vulnerability to obtain identity information. Businesses should strive for more holistic safeguards that extend across multiple domains.

What to Expect in 2008

- *Identity theft is likely to remain a topic of concern for consumers and the media.*
  Expect customers increasingly to demand information regarding the steps that are being taken to safeguard their information.

Human

> "Amateurs hack systems, professionals hack people."
>
> —Bruce Schneier, cryptographer, computer security specialist, and writer

Despite significant advances in security technologies, policies, and awareness, human beings remain the single most vulnerable aspect of security. Major trends in the area of human security issues in 2007 included multiple breaches resulting from human error, and huge increases in phishing and social engineering attacks.

Human Error Leads to Major Security Breaches

The notion that accidental disclosures resulting from human error and poor controls on sensitive information can cause just as many problems as malicious attacks was reinforced in 2007. Incidents included:

- Revelation in April that a U.S. Census Website had listed the Social Security numbers of 63,000 people for 11 years
- Printing of Social Security numbers on tax booklets mailed out to 171,000 Wisconsin taxpayers in January
- Improper disposal of personal and financial records by J.P. Morgan Chase, in which trash bags containing financial records were found outside the offices
- U.S. Internal Revenue Service (IRS) audit in July revealing that more than 50 percent of IRS employees disclosed passwords to callers posing as technicians
- Accidental deletion of an Alaska Department of Revenue hard drive containing information related to a US$38 billion account, requiring a recovery effort that cost more than US$220,000.

Phishing and Social Engineering on the Rise

Criminals have become more effective than ever at enticing people to disclose sensitive information or put their systems at risk. Attacks employed a broad range of techniques, often using current events and emotionally engaging subjects to dupe users. Examples included:

- The Infostealer.Monstres Trojan, which captured an estimated 1.6 million personal records from Monster.com; the records were used to launch a massive targeted phishing campaign
- An iPhone phishing Trojan that launched a popup window at major search engines, redirecting users to a malicious Website
- A rash of fraudulent Websites and spam e-mail messages that emerged in the wake of the Virginia Tech shootings
- Multiple attacks that targeted employees of the U.S. Department of Transportation via e-mails, false job postings, and advertisements
- A spoofed IRS e-mail that claimed recipients were the subject of a tax audit and contained links to malicious code
- An e-mail phishing campaign that targeted customers of Nordea, a Swedish bank, resulting in the theft of more than US$1 million from customer accounts
- A phishing scam that targeted 60,000 MySpace users and directed them to a malicious Website

Key Recommendations

- *Employ strong security policies governing user behavior.*
  The only way to safeguard against human vulnerabilities is to implement strong policies regarding data access control, inspection points, passwords, and network security, and to train on and reinforce those policies continually.
- *Educate users about social engineering risks.*
  Organizations must educate users through awareness and training to recognize social engineering attacks. They must continually reinforce the importance of not trusting e-mails, Websites, advertisements, and other communications from unknown or untrustworthy sources. For more information on building effective security awareness, education, and training programs, visit: http://www.cisco.com/web/about/security/cspo/awareness/index.html
- *Don't assume that an attack is what it seems.*
  Increasingly, attackers are looking to steal information not just for the value of the information itself, but for use in targeted phishing and social engineering attacks. Even if a security breach seems minor, organizations should evaluate whether any disclosed information might be used for such purposes and warn users.
- *Use technologies that slow down attacks.*
  Antispam tools, "gray-listing" of e-mails, URL blacklists, and other technologies can slow down attacks and provide organizations with more time to identify and respond to e-mail- and Web-based threats.

What to Expect in 2008

- *Expect phishing and social engineering attacks to increase.*
  As long as attackers can trick users easily and profitably, these types of attacks will continue to play a major role in criminal enterprises.

Geopolitical

> "We only need to be lucky once. You need to be lucky every time."
>
> —The Irish Republican Army in a statement to Margaret Thatcher after a *failed assassination attempt*

Several geopolitical trends in 2007 had an impact on business and security considerations. Dominant trends included the ongoing threat of terrorism around the world; the continuing ascendance of developing economies such as China, India, and Brazil; a growing global focus on environmental issues; and the growing recognition of cyberspace as a theatre for military action and international espionage.

Continuing Threat of Terrorism Worldwide

As was the case during the last several years, there were multiple terrorist events around the world in 2007. Significant events included:

- Airport car-bomb attack in Madrid, Spain
- Train bombing north of Delhi, India
- Disruption of planned Al Qaeda attack on Telehouse Europe headquarters with the goal of disrupting Internet service in the United Kingdom
- Car-bomb attack on Scotland airport terminal
- Disruption of planned car-bomb attacks in London
- Bombing of Tour de France route in Spain
- Disruption of planned Al Qaeda attacks in Germany
- Suicide bombing of former Prime Minister Benazir Bhutto's motorcade in Karachi, Pakistan

These events reinforce that terrorism remains a real concern for organizations in a wide range of industries around the world. And as attacks in Western Europe demonstrated in 2007, any business interest identified as a Western enterprise anywhere in the world is at risk of terrorist attack.

Continued Ascendance of Developing Countries on the International Scene

Globally, developing economies such as those in China, India, and Brazil, and emerging economies such as many in the Middle East, Eastern Europe, and Africa, continued to grow and expand in 2007 at rates that exceeded the developed world. For example, China's economy grew at 11 percent or better throughout 2007. This rapid growth had cross-current effects; for example, pushing up prices in China and raising concerns that China's stock markets may be in for a hard landing. At the same time, however, China's continued robust growth has been good news overall for the world economy—cushioning world markets, for example, during the mid-2007 credit crisis. These developing world trends are affecting all businesses and will likely continue to do so for the foreseeable future.

Significant geopolitical events concerning the developing world during 2007 included:

- Nationalization of previously foreign-owned oil projects in Venezuela by Venezuelan President Hugo Chavez
- Continuing instability in Thailand and continuing threat from Muslim insurgents in the south of the country
- A demonstration by the Chinese military of its capacity to shoot down a satellite, reinforcing the reality that space-related technologies are vulnerable

- Ongoing safety issues with products originating from China, causing businesses worldwide to re-evaluate relationships with Chinese manufacturers
- Complaints filed with the World Trade Organization by the United States regarding weak piracy law enforcement in China
- China's launch of a lunar probe
- Reappointment of Chinese President Hu Jintao, assuring his continued tenure until 2012
- Violent crackdown on dissidents in Myanmar

Growing Global Focus on Environmental Issues

The year 2007 saw a turning point in a global focus on environmental issues and concerns, which dominated the media and public consciousness. As more countries and industries adopt "greener" policies to promote environmental conservation, businesses are becoming increasingly conscious of the environmental ramifications of their operations, presenting both a significant market opportunity and significant potential costs to retrofit less environmentally friendly technologies.

Major environmental trends in 2007 included:

- Increasing market advantages for businesses that underscore the environmental benefits of their products or demonstrate a commitment to lower environmental impact
- Growing risk of major weather events worldwide, increasing business vulnerability everywhere
- Lack of clean water and poor air quality in China, which is affecting productivity and increasing the risk to businesses operating or engaged in partnerships there

Emergence of Cyberspace as a Major Theatre for War and Espionage

As industries, governments, and individuals have become more connected over the past decade, cyberspace has become an increasingly significant domain for military and espionage activities. Examples in 2007 include:

- The creation of a "Cyber Command" by the U.S. Air Force, demonstrating the U.S. military's recognition of cyberspace as a major area of military focus, both in terms of defense and as a potential launching point for offensive action
- Growing evidence of international espionage as the motive behind network attacks in the United States, Australia, New Zealand, the United Kingdom, Germany, and elsewhere
- Arrests and convictions of a large number of individuals who were caught stealing sensitive intellectual property and selling it to foreign governments
- Accusations by political opponents of Russian president Vladimir Putin that the Kremlin had orchestrated network security attacks against them
- Network security attacks in Estonia, which brought down many government and financial computers

Key Recommendations

- *Ensure that contingency plans address the possibility of a network security attack.* Businesses operating near potential high-profile terrorist targets need to consider the possibility of being attacked or facing collateral damage from an attack. Businesses that outsource or maintain branches in countries that may be politically unstable, or that host groups that are hostile to the corporate culture or mission, should be particularly vigilant.
- *Adopt a global business perspective.* Small and especially midsize businesses should be prepared for the reality that events around the globe will increasingly affect their business operations. For U.S. businesses, emphasizing the international aspects of the business—and playing down purely American aspects—may not only be good public relations, it may also keep assets overseas more safe.
- *Protect against unsafe products.* Businesses are responsible for the safety of their products, regardless of where they were produced (e.g., by an offshore subcontractor). Businesses that rely on products manufactured overseas should re-evaluate the safety of products and manufacturing processes to protect against legal liability and damage to the company's reputation.
- *Recognize espionage as a real threat.* Organizations that control sensitive trade or government information should recognize that the threat of international and industrial espionage is real. Organizations should incorporate strong security policies and procedures to safeguard sensitive data and continually monitor systems and personnel.

What to Expect in 2008

- *Expect increased spending by governments on Internet and network technologies.* With cyberspace becoming a more prominent venue for military activity, expect government technology budgets to increase substantially.
- *Expect increased spending on "green" technologies.* As more organizations strive to implement environmentally friendly business practices, businesses should expect to see growth in technology retrofitting that will present both a market opportunity and significant potential costs.

Conclusion

> "In a world in which the total of human knowledge is doubling about every ten years, our security can rest only on our ability to learn."
>
> —Nathaniel Branden, psychotherapist and philosopher

This security report represents Cisco's extensive security experience, and its diverse security and business operations around the globe. The vast number of businesses, governments, and industries with which we work—as well as the worldwide scope of our internal network—means that we are constantly learning valuable security lessons. Through publications such as IntelliShield Cyber Risk Reports, as well as reports such as this, we strive to provide our customers with the knowledge we gain, and ultimately, to help improve organizational security around the world.

At the highest level, when reviewing the trends from the past year, Cisco security experts have drawn the following conclusions:

Threats are evolving before our eyes.

Security threats are becoming much more targeted. Attacks are increasingly being launched for mercenary motives, as opposed to the "cybervandalism" of the past. This change significantly raises the stakes in the ongoing battle against network security attacks. As attackers increasingly target objectives with monetary value, they will devote more effort and resources toward devising more creative, difficult-to-detect attacks.

What we can do about it:

Security professionals and businesses need to focus more on which targets in their organization will be most attractive to attackers, in addition to which avenues attackers are most likely to exploit. It is also important to understand that threats follow usage. Every time a new type of application, communication, or collaboration emerges, threats will naturally evolve to target that new area. In the immediate future, security professionals should be paying close attention to emerging communication and collaboration tools—particularly mobile tools—as this will likely be the next area of focus for attackers.

The concept of "information security" is evolving.

As the numerous thefts of identity and financial information that occurred in 2007 demonstrated, modern businesses need to pay just as much attention to what is leaving their domain as to what is entering. In the past, businesses and security professionals were perhaps too confident that as long as they could block malicious traffic trying to enter the network, the business was safe. This is no longer the case. While businesses must be as vigilant as ever about protecting the infrastructure, they must also focus more efforts on protecting the information in their environment that is of value—from both internal and external threats. Unfortunately, many businesses are at a loss for how to do this effectively. They are looking to industry leaders to devise better solutions.

What we can do about it:

While solutions have emerged in specific areas (for example, thoughtful use of encryption, inspection points, data controls, and compliance standards such as PCI), business customers are still waiting for a comprehensive answer that extends across all areas of vulnerability. One of the biggest hurdles the industry must overcome is the lack of a sense of ownership of this problem. Just as we are urging customers to adopt a more holistic approach to security, vendors themselves need to break down the barriers between their traditional "silos" of expertise. Customers don't

care if a vendor traditionally focuses on the network or on wireless or on applications. They want to know how vendors are going to help them protect their data—across their entire environment. Fortunately, the industry is increasingly recognizing this problem. Within the next 12 to 24 months, we expect to see leading vendors taking a much more aggressive stance in providing more comprehensive, holistic security that extends throughout infrastructure, applications, and data.

Education must become a bigger focus.

Security professionals and businesses alike seem to agree that user education and awareness are the most effective defense against threats. And yet, across the industry, many businesses spend more every year on everything except education.

What we can do about it:

Both businesses and security vendors need to devote more of their resources toward education initiatives, including developing new and more creative educational approaches. Across the industry, vendors and businesses should also consider sharing education and training programs the same way we now share new threat information. At Cisco, for example, we make our security training and awareness programs available at no charge for any company or educational institution to use. For more information on Cisco security awareness, education, and training programs, visit http://www.cisco.com/web/about/security/cspo/awareness/index.html.

As a society, we also need to begin taking a generational approach to security education. As the world continues to become more closely interconnected, one of the best security investments we can make is institutionalizing computer security training in schools, so that individuals can learn, from a young age, how to protect themselves. More businesses should also consider joining awareness-building efforts such as the National Cyber Security Alliance in the United States.

Revolutionary answers may be required to thwart evolving attacks.

While businesses and the technology industry as a whole have become more effective at identifying and patching vulnerabilities, this inherently reactive approach to security may not be enough to protect us from tomorrow's threats. In the past, even when security analysts were identifying new OS vulnerabilities every week, there were still only a small number of operating systems actually in use. Today, as applications increasingly become the target, we need to recognize that there are more than one million application vendors registered around the world, creating a much more complex problem.

An even greater concern is the continued assumption that organizations will always be able to patch vulnerabilities as they are discovered. As we move steadily toward an environment in which more services need to provide 24x7 availability, it becomes ever-more difficult to patch and reboot machines. Increasingly, IT teams will be faced with a difficult decision: Do we live with a vulnerability because we can't take our machines offline right now, or do we patch and suffer a service outage that may affect our customers? That we are moving toward a situation in which service availability and network vulnerability are fundamentally in conflict should tell us that we need to consider new approaches.

What we can do about it:

In the short term, businesses should consider augmenting signature-based solutions with more proactive threat defense approaches. The ability of Cisco Security Agent, for example, to identify and block suspicious OS behavior—without having to identify any specific attack—has been an enormous benefit for many Cisco customers, and for Cisco itself in our ability to protect our own network.

In the long term, however, both vendors and businesses need to adopt a more holistic, proactive approach to security. Security should be fundamentally integrated into every aspect of the environment. When building a network, businesses should focus not just on performance and capabilities, but on the infrastructure's ability to collaborate, inspect, adapt, and self-heal, from end to end. When the network plays the central role in enforcing more holistic security, businesses are better protected and can better respond to future needs. For example, if a business historically approached wireless security, network security, and voice security separately, it faces a major new security problem when the company adopts a wireless unified communications solution. By taking a more systemic, architectural approach to security, corporations are inherently better prepared for new applications and forms of integration that will emerge.

Part of creating the intelligent, adaptive, self-healing environment that Cisco refers to as a "self-defending network" involves keeping IT infrastructure, operating systems, and applications current. Using an up-to-date infrastructure not only reduces vulnerabilities—it also increases the number of tools and techniques that corporations can use to protect themselves.

Finally, proactive security also means continually re-evaluating the state of the environment's defenses. Even conscientious security professionals and organizations can become complacent. But conditions are changing constantly—both internally, in terms of new applications, services, and users, and externally, in the form of continually evolving threats. Businesses cannot assume that just because security was considered strong the last time it was evaluated, it is still strong. Corporations should institutionalize periodic security posture assessments and architectural reviews, and perform such evaluations every few months.

Better Solutions for Responding to Evolving Security Threats

All of these issues will present new challenges and new business opportunities over the next several years. But one overarching aspect of security that is already evolving to deliver better solutions for customers is security intelligence. In the past, organizations' lack of up-to-date knowledge about new threats left them in the dark about the ways in which their environments might be vulnerable. Today, they have the opposite problem: more security alerts coming in than IT groups know what to do with. Modern organizations need ways to quickly identify when an alert specifically affects their business and environment, and what they can do to fix it when it does.

Fortunately, new solutions are emerging to help businesses manage and respond to security information more effectively. The Cisco Security Center provides up-to-the-minute information on current threats and vulnerabilities, as well as links to patches and remediation solutions. Going beyond basic problem reporting, the Cisco Security Center provides details not only on the nature of newly identified threats, but also on the ways businesses can use their Cisco infrastructure to protect themselves.

To find out about the latest security threats and the ways you can use your Cisco network to remediate them, visit the Cisco Security Center at http://www.cisco.com/security.

For more information about the Cisco Security IntelliShield Alert Manager Service, visit http://www.cisco.com/go/intellishield.

For details on the Cisco portfolio of intelligent security solutions and services, visit http://www.cisco.com/go/security.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**

Printed in USA C02-443493-00 12/07