



Cisco 2010 Midyear Security Report

The impact of global security threats
and trends on the enterprise





Web 2.0, mobility, virtualization, and other dramatic shifts in how we communicate and collaborate are carving out a new landscape for business and for enterprise security. The *Cisco® Midyear Security Report* examines these changes and their impact on the enterprise, and highlights other significant trends and threats creating security challenges for organizations worldwide. The report also includes recommendations from Cisco security experts designed to help enterprises strengthen their security.



2 Enterprises and the Tectonic Forces of Change

Cisco Study: Collaboration Critical to Employee Success

4 The Technologic Shift: The Proliferation of Mobile and Connected Devices

The Mobile Device Onslaught

What's Disrupting the Enterprise? Consumerization of IT

Risk Alert: IP-Addressable Devices: Who's Listening to Your Network?

What's Disrupting the Enterprise? Mobility

8 The Economic Shift: Virtualization of Operations

What's Disrupting the Enterprise? Virtualization

10 The Demographic Shift: The Role of Collaboration and Social Networks

Social Media for Enterprises: Upside and Downside

It's 3 p.m.—What Are Your Employees Doing? Tending Their Virtual Fields

What's Disrupting the Enterprise? Social Media

13 Worldwide Government Trends: The Impact on Business

Multiple Governments, Multiple Stances on Security

Global Security Guidelines: Should Business Become a Player?

U.S. Government Update

Privacy Issues Moving to the Forefront

16 Taking Action to Reduce Innovation Gaps

Criminals Now Protecting *Their* Intellectual Property

The Spread of IPv6 and Domain Name System Security

Risk Alert: A "Perfect Storm" of Technological Change

Explosive Growth in Connected Devices and Applications—Along with New Threats

20 Insight from the Security Researchers: Hackers Are Choosing Their Own Adventure

Risk Alert: Advanced Persistent Threats

Risk Alert: The Downside of Being a VIP (or Just Working for One)

Small Targets, Big Rewards

What Keeps Your IT Security Team Awake at Night?

25 Five Ways Enterprises Can Strengthen Their Security by 2011

30 Security Trends: Midyear Notes

32 Cisco Security Intelligence Operations

Cisco Security IntelliShield Alert Manager Service



Enterprises and the Tectonic Forces of Change



The business world continues to evolve due to spectacular revolutionary forces that are changing the way we work, live, learn, and play, and how we communicate and share information. These changes aren't something enterprises can choose to take part in or ignore; in fact, they're already having a profound impact on your business and your life at this very moment, whether you are unaware of or welcome the change.

These changes are part of the dramatic shifts—"tectonic forces"—that are making it essential for businesses to rethink their approach to enterprise security. Gone are the days when a network firewall would deter teenagers looking to hack into corporate databases for the challenge, notoriety, or for the fun of it. Now, serious and well-resourced criminals with business plans are intent on stealing both personal data and business intelligence they can sell—and perimeter-based security alone cannot stop them.

What are these forces? Primarily, the rise of social networking, the enthusiastic adoption and proliferation of network-connected devices, and the embrace of virtualization are altering the threat landscape. Time travelers from the 1970s would barely recognize today's workplace.

They likely would be most surprised about not having to go to a specific location, such as an office, to get their work done. People are increasingly dependent on smartphones and other mobile devices for everyday communication, collaboration, and work, and are using this technology more often beyond the traditional office and network boundaries.

Users also are relying on social networking services such as Facebook and Twitter, online collaborative work tools like Google Docs, and software-as-a-service (SaaS) applications that don't live on the company's servers. Even if an organization attempts to ban access to certain web services or sites, savvy users will find a way around these attempts to continue to access the services they find useful—and believe are necessary to do their jobs.

How do these changes affect an enterprise's plans to protect its data? Since workers now collaborate and share vital information outside of the workplace, security that's limited to the network edge is bound to fail. The emerging "borderless network" has no defined edge or boundary; instead, it has many borders that are constantly changing. And for the most part, enterprises cannot effectively control the myriad devices/endpoints on the network.

This hastens the need for a new model for security that acknowledges the movement of corporate data among offices, smartphones, workers' home computers, laptops, Internet cafes, and any other place where employees choose to work. Workers want access to customer lists and project data from their iPhones and BlackBerry devices, whether they are sitting in the coffee shop near their office

or waiting at an airport gate halfway across the world. The enterprise is tasked with granting them this “borderless” access, while ensuring the data stays safe.

Effective controls are needed to address the potential security and productivity issues that can arise from uncontrolled access to social networking services. New data from Cisco shows that employees accessing interactive games via Facebook can spend an hour or more a day playing these games (see graphic on page 11 for details). To manage security and productivity, organizations should enact clear policies regarding access to social networking sites; in addition, they can consider limiting access to social networking to those employees whose jobs require it (for example, PR and marketing functions).

There are technical challenges—and solutions—for this emerging environment. For a security solution to be effective, a change in mindset must take place. Too often, enterprises view security as an add-on, rather than a business enabler. IT departments tend to operate on the

defense against security threats, instead of on the offense with long-range plans for managing security.

In addition, employees are too often categorized as “part of the security problem” and not willing participants who can play a key role in improving an organization’s security process. Fearful of data loss or theft, enterprises may unilaterally bar employees from accessing webmail or social networking sites, or will forbid any smartphone that’s not approved for use by management. This way of thinking does little to improve security—as stated, workers will figure out how to circumvent rules—and makes for a resentful workforce.

While some businesses may not see the value in making the technological and cultural shifts necessary for modern security, today’s threat landscape demands more comprehensive security to protect against criminals who operate online and are armed with the same sophisticated software tools (and talents) claimed by the most tech-savvy businesses.

Criminal enterprises are entirely professional in their approach to stealing sensitive information. They are driven to succeed and receive the payoff. They also have key advantages that most network security administrators do not: plenty of time and resources to accomplish their tasks.

Businesses are a prime target for today’s online criminals, which is why the *Cisco 2010 Midyear Security Report* is tailored for the business community. In particular focus are the three “tectonic forces” of change, which are dramatically altering the cybersecurity landscape:

- **The technologic shift:** The proliferation of mobile and connected devices
- **The economic shift:** Virtualization of operations
- **The demographic shift:** The role of collaboration and social networks

This report also examines another significant challenge organizations must face in the midst of all this dramatic change: responding to the demands of still-evolving security regulations and expectations in the countries where they conduct business.

Some enterprises may find that meeting today’s security challenges is a daunting task, but many will find it’s worth the effort. Effective security practices are an asset that can strengthen a company’s reputation and competitive edge. The good news is that viable solutions do exist.

Cisco Study: Collaboration Critical to Employee Success

Today’s employees expect to collaborate extensively with their colleagues—and believe it’s not just beneficial, but essential to their careers and to the business. In a recent study, Cisco surveyed employees at midmarket and enterprise businesses in the United States and found that when workers embrace collaboration, they do so wholeheartedly. More than 75 percent said collaboration is critical to their success on the job; more than 90 percent said collaboration makes them more productive.

The study divided respondents into four categories. Workers identified as “Collaboration Enthusiasts”—those who believe collaboration is a key business differentiator—use an average of 22 tools, including social networking sites, blogs, and wikis, to connect with colleagues. Respondents in the “Collaboration Laggard” group use far fewer such tools, often because their company doesn’t make them available.

Competitive, entrepreneurial businesses should consider the type of work environment they want to foster and employees they would like to attract. If businesses

intend to champion collaborative work processes, they must welcome the use of tools and solutions that may feel uncomfortable, from a security standpoint.





The Technologic Shift: The Proliferation of Mobile and Connected Devices



Workers are reaching unprecedented levels of productivity because they are more connected to each other and the information they need than ever before. In the past, individuals were first exposed to “cutting-edge” technology in the workplace, and it took years for business-world innovations such as computers and copiers to become fixtures in the home environment. But the consumerization of IT—where new technology is adopted by consumers even before it is introduced into the enterprise—has changed the direction of technological innovation. In fact, many individuals today have more computing power in their homes than in the workplace.

While having a more efficient workforce is obviously a positive for businesses, the proliferation of not only mobile, wireless devices—but also *connected* devices—in the enterprise creates security challenges for IT departments. Unsupported laptops and smartphones (such as RIM BlackBerry devices, Google Android phones and the Palm Pre), consumer devices (such as Apple iPods and iPads), and IP-addressable devices (ranging from digital cameras to digital printers) are being *pushed* aggressively into the workplace by employees at all levels, from recent college graduates to C-level executives. Users embrace new technology in their personal lives and resist the

idea that they can't use the same devices and applications at work—even if their company's security policy and the IT department enforcing these rules forbid it.

However, the trend toward consumerization of IT is not just about workers demanding that they be allowed to use trendy new devices for business instead of bland, corporate-issued mobile phones or laptops. This is about employees bringing a range of devices into the enterprise that they believe they must have access to for optimal productivity. Consider what the average young adult (a member of the future workforce) will “need” to take to college this fall: a laptop or netbook, a smartphone, an MP3 player, gaming console, digital video recorder, video camera, and digital camera. And all these devices can connect to the Internet—and more often now to each other, as well.

The Mobile Device Onslaught

It was only a few years ago that the typical consumer or office worker had only one connected device—and, in most cases, it was a Microsoft Windows PC. But dramatic advancement in both communications technology and consumer electronics means that we are living and working in an infinitely more complex environment surrounded by a diverse range of devices that can easily connect to the Internet, to each other, and, quite possibly, to your company's network.

IT groups struggle with mobile device management because there are so many devices in a variety of form factors in employees' hands—and with them comes an endless array of software platforms, mobile applications, and

service providers. Users also constantly switch devices to take advantage of the latest technology development. And inevitably, they lose devices—or allow them to be compromised or stolen. It would be ideal, of course, if IT could manage all mobile devices in use in the enterprise through their entire life cycle, but due to the consumerization of IT, they don't have that control. Nor does IT have the resources to even attempt to micro-manage each individual device that is not issued or supported by the enterprise.

There is no questioning IT's challenge: The number of mobile and wireless-enabled devices in use worldwide is growing exponentially—as are the number of remote and mobile workers. In the United States alone, more than 257 million data-capable devices were in circulation at the end of 2009, compared with 228 million at the end of 2008, according to CTIA, a nonprofit wireless industry organization.¹ Research firm IDC predicts that by 2013, the number of mobile devices—smartphones and wireless devices—accessing the Internet will surpass 1 billion.²

Enterprises can expect smartphones to be a primary focus for attackers because of their popularity—and the fact that they are becoming *the* productivity and communications device of choice for many workers. Infonetics Research anticipates that smartphones will be the only mobile phone segment to post double-digit annual revenue growth over the next five years. And according to Gartner, "Most users in 2010 will use a PC as their primary Web access device and their phone as a secondary access device. However, as take-up of smartphones spreads globally, there will come a point in 2015 when the mobile phone will overtake the PC as the most common primary device for Web access worldwide."³

To be sure, serious threats—such as worms and malicious code—are in the future for mobile devices. The first iPhone worm, "Ikee," appeared late last year, written by an unemployed programmer as a prank. It was a small-scale incident: The worm targeted only Australian users with "jailbroken" smartphones (phones modified to run unauthorized software), replacing the device's wallpaper with an image of 1980s pop star, Rick Astley.⁴ But more sinister actions are likely not far behind: Researchers at Rutgers University recently warned of rootkits that can undermine a smartphone's operating system and allow criminals to eavesdrop

1 "CTIA-The Wireless Association Announces Semi-Annual Wireless Industry Survey Results," media release, March 23, 2010, www.ctia.org/media/press/body.cfm/prid/1936.

2 "IDC: 1 Billion Mobile Devices Will Go Online by 2013," by Agam Shah, CIO.com, December 9, 2009, www.cio.com/article/510440/IDC_1_Billion_Mobile_Devices_Will_Go_Online_By_2013.

3 *Gartner's Top Predictions for IT Organizations and Users, 2010 and Beyond: A New Balance*, G. Gammage, Gartner, Inc., December 29, 2009.

4 "Jailbroken iPhones: set free to get mugged," by John Cox, John Cox on Wireless, NetworkWorld.com Community, November 10, 2009, www.networkworld.com/community/node/47588.

What's Disrupting the Enterprise? Consumerization of IT

Devices and applications that are first adopted by users outside the work environment have made great inroads within businesses—but not without raising tough questions about their impact on enterprise security. Use of technology that is not supported by the enterprise may violate corporate security policies and may pose a risk to the organization's compliance with regulations related to data security.

✔ ACTION ITEM:

Set strict controls for access to business data.

For many organizations, refusing to allow employees to use the technology they prefer in the workplace is not a sustainable approach to security. Still, not all devices are appropriate for everyone in the enterprise. Do all employees, from the C-suite down through the organization, need access to all business data on their smartphones? It is unlikely. Businesses should ask tough questions about who truly needs such access, since there is benefit in limiting borderless access to information.

Start conservatively by restricting as much access as possible, and then relax requirements on a case-by-case basis. In addition to restricting access by users, consider limiting access by data—for example, some intranet pages



should be accessible to everyone using an approved smartphone, while certain customer relationship management (CRM) applications should not be accessible at all through this vector. Talk with your security vendor about solutions designed to help protect the company's network and data, regardless of what device an employee uses to gain access to the corporate network.

on conversations, steal personal information from phone directories, and even track a user's whereabouts.⁵

Many criminals will likely spend little time on individual users, though, and instead focus on using their mobile devices as a way to gain access to corporate networks, compromise hosts, and harvest sensitive business data (see *Insight from the Security Researchers: Hackers Are Choosing Their Own Adventure*, page 20). Cybercriminals are more focused today on overcoming network security than simply defeating a device—the goal is to get into the network and stay there for as long as necessary or possible.

Mobile devices represent just one potential inroad into the network for those intent on doing harm. There are more worries for businesses than smartphones: Every connection point is vulnerable—from rogue hotspots to insecure service providers, including webmail, application, portal, and cloud service providers. Complicating matters is that many devices are now capable of sharing data with each other wirelessly, and with little effort on the part of users to make a connection.

Wi-Fi Direct technology, for example, built into many consumer devices now entering the market, allows consumer devices to establish connectivity through Wi-Fi, other devices (including peripheral devices, like printers), or another network without any setup—or even to create a Wi-Fi “hotspot.” Essentially, every supported device becomes a mini access point that can connect with other Wi-Fi-enabled devices within a 300-foot range.

These ad hoc connections are convenient for end users, but they create obvious soft spots for data security—and underscore IT's challenge in maintaining adequate visibility into and control of the highly populated and active endpoint landscape in the enterprise. It should be noted that the Wi-Fi Direct specification contains security features to prevent peer-to-peer devices from compromising corporate networks.⁶ Still, the onus is on enterprises to make sure that WPA2, an encryption technology that protects data flowing between Wi-Fi radios and access points, is enabled on the network.⁷

▲ RISK ALERT: **IP-Addressable Devices:** **Who's Listening to Your Network?**

The concept of a “networked refrigerator” that's connected to the Internet may seem like a running joke among watchers of the Internet's infiltration onto a host of devices, but at a time when cars with Internet-enabled dashboard screens are being introduced, the idea of more and more business devices that can communicate on a network doesn't seem so far-fetched. And as wireless devices beyond the usual desktop and laptop computers start connecting to corporate networks, the threat window only grows: Criminals need to find only a single unguarded “in” to begin snooping into a network.

It is not difficult to find the open doors. Wireless printers, for example, which are now commonplace in the enterprise, can retain digital images—a potential boon for data thieves. And what about the digital camera that can seek a connection to a laptop that happens to be connected to a corporate network? The camera and the laptop establish a wireless connection, making it possible for the user of the digital camera to “leapfrog” directly into

the corporate network. The data being passed between wireless devices is also vulnerable, and could easily be hijacked and used inappropriately.

The variety of endpoints that are capable of being connected, or are already connected, is astonishing.

This interconnectedness will escalate, as will the effects it will have on our networks. In just a few years, every door lock, card reader, video camera, vehicle, power meter, and light switch will have an IP address—at least in the business world. Therefore, from a security standpoint, it will become increasingly important—within the enterprise and within our homes (since many of us are now mobile or remote workers, too)—to segment and firewall different classes of devices in a network.

Enterprises also should keep in mind that their “smart” office devices can be sources for data loss in other ways—no wireless connectivity required. For instance, data thieves may only need to make a small investment in a few used digital copiers to reap a big return in their hunt for sensitive data: An investigative report by CBS News showed how easy it is to retrieve tens of thousands of documents from digital copiers that have not had their hard drives sanitized prior to resale. Among the information found: Design plans for a building near “Ground Zero,” the site of the 9/11 terrorist attacks in Manhattan, and 95 pages of pay stubs with names, addresses, and Social Security numbers for employees of a New York construction firm.⁸

5 “Smart phone under threat of attacks,” by Alexey Kushnerov, TheTicker.org, March 1, 2010, www.theticker.org/about/2.8220/smart-phone-under-threat-of-attacks-1.2174454.

6 “New Wi-Fi Direct Gets Peer-to-Peer Connections,” by David Coursey, PCWorld.com, October 14, 2009, www.pcworld.com/businesscenter/article/173669/new_wifi_direct_gets_peertopeer_connections.html.

7 Wi-Fi Alliance FAQs, www.wi-fi.org/knowledge_center_overview.php?type=2.

8 “Digital Photocopiers Loaded with Secrets,” by Armen Keteyian, CBS News, April 15, 2010, www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml.

What's Disrupting the Enterprise? Mobility

Data is on the move like never before. According to the *Cisco Visual Networking Index (VNI) Global Mobile Data Forecast, 2009–2014*, mobile data traffic will continue to double every year through 2014 (with video, the bandwidth hog, representing more than 66 percent of the world's mobile data traffic).⁹ Moving that data: smartphones and portables (91 percent), according to Cisco research.

Data transcending borders and boundaries can undermine even the best-laid plans for corporate security. Currently, however, most enterprises mold their mobile security strategies around compliance measures—such as United States (U.S.) requirements like the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS)—relating to how personal information, both stored and in motion, is protected by businesses.

Government regulations, the lawsuits, fines, and reputational damage that can result from noncompliance, and security breaches are all significant motivators, of course, but companies need to think beyond these requirements if they want to embrace mobility fully as a way of working and exchanging information. Compliance does not equal security—nor does it take into account all sensitive information that an enterprise may want and need to protect.

✓ ACTION ITEM:

Create a formal corporate policy for mobility.

Step 1: Find out how mobility is happening in the corporate environment—and why—to build appropriate security parameters. Understand what the business value of mobility is for the enterprise. The approach will vary by company and industry (for example, an educational institution's security concerns around mobility are likely to be quite different from those of an energy company with a nuclear facility).

Step 2: Create an acceptable-use policy that outlines the devices that are supported by the enterprise. Outline what disciplinary actions may result due to noncompliance with corporate policies relating to the use of mobile devices. Explain why certain devices are not permitted in the enterprise (and if/when that policy might change).

Step 3: When crafting a policy, keep in mind that it should be flexible enough to cover both immediate and future security concerns. Take into consideration what the organization might need to compete in the future and attract top talent—particularly from the very mobile, very connected Generation Y.

Step 4: Educate the workforce. Communicate—and enforce—the policy across the organization. But keep in mind that secure mobility is not just about enforcing acceptable-use policies from a human resources or legal standpoint: It's also about the safety of the network.

Step 5: Manage the device life cycle. You may not be able to manage every mobile device in the enterprise, but you can inventory every device you do control. Note the level of access of the user. Can the user access sales figures, personnel files, or customer data? Through this process, create a record of who is accessing what information, with what device (or application), and for what reason.

In addition, make sure you have the ability to lock and/or wipe clean a device automatically and remotely after employment termination or if a device is lost or stolen—a critical security measure. Consider the example of an HR department staff member who loses a device with employees' personally identifiable information saved on it. That data, once exposed, could be used inappropriately by identity thieves and can create serious legal and disclosure woes for the company.

Mobile security also needs a system-level approach that goes beyond setting acceptable-use policies. Enterprises should implement tools that allow visibility into wireless environments and detect security threats as they emerge so they can take swift action.



⁹ *Cisco Visual Networking Index (VNI): Global Mobile Data Traffic Forecast Update, 2009–2014*, www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.



The Economic Shift: Virtualization of Operations

When news about the virtualization of commonly used business solutions makes the front page of major newspapers' business sections on a regular basis, it's time to acknowledge that this trend is having a significant impact on the enterprise.

This is largely good news. Businesses can afford to gain access to services they might not otherwise be able to purchase as on-premises solutions. They can free up capital to use for other parts of the business. They can make greater strides toward "going green," reducing office square footage and travel costs. And workers don't need to be in the office to access the systems they need to be productive.

The downside of virtualization of business solutions lies in the security of the data. Where is information going and who has access to it? How strong are access controls? What protections are built-in to prevent breaches?

However, this type of virtualization does offer some resiliency that may aid security. For instance, if the workplace is disrupted because of an attack on systems or structures (at the farthest end of the scale, a terrorist attack), employees can continue with day-to-day operations from anywhere they happen to be—assuming, of course, the cloud infrastructure itself wasn't attacked. Since data is not resident on end devices, such as laptops or smartphones, theft or loss of equipment isn't as dire a scenario for businesses. In addition, building scalable policies around upgrades is easier in the cloud environment. (See page 9 for key questions to ask when adopting the use of cloud computing solutions.)

What's Disrupting the Enterprise? Virtualization

As with consumer devices, virtualization invites enterprises to grant visibility and data access to a wide swath of workers, and often, customers and partners. Enterprises must learn how to manage this new twist on technology and available assets.

The way to mitigate the potential risks of virtualization is to ensure granular, per-user application and data policies are enforced on virtualized systems. Vulnerability management can help ensure that easy-to-fix security gaps aren't ignored, and disaster/continuity planning can help make use of virtualization's advantages for keeping an enterprise operational.

From a security and data protection standpoint, virtualization demands that enterprises change their perspectives toward identity, compliance, and data. To address disruptive trends such as mobile device adoption, the borderless enterprise, software virtualization, and the concept of "any device, anywhere, anytime," enterprises must implement:

- Identity life-cycle management, "persona" reconciliation, and authentication convergence planning capabilities
- Data-centric policy shifts, such as greater focus on understanding data in motion and data governance
- Software and asset management, identity-enabled networking service/platform cost control and recovery, and service management models
- Secure access for partners, as more businesses outsource core business functions to outside organizations

It's also a good idea to negotiate comprehensive service level agreements (SLAs) with cloud providers and retain the capability to audit those services as necessary.

✔ ACTION ITEM:

Invest in tools to manage and monitor cloud activities.

Virtualized platforms do allow for new avenues of data loss; for instance, a virtualization administrator can perform certain actions, such as removing data or shutting down virtual machines, without the enterprise being aware. In the old "physical world," these types of activities would have required the addition of hardware devices, or the installation of software on the operating system itself.

While some loss of control over data is inevitable with virtualization, businesses should take advantage of technology that provides some visibility into systems not based entirely on-premises. Solutions on the market include those that offer "health checks" and performance dashboards to help IT manage cloud services. Organizations also should schedule yearly reviews of where data resides.

Action Plan for Adopting Cloud Computing

Businesses are allowing many audiences—employees, partners, vendors, and customers—to benefit from working with solutions based on the cloud computing model. Below are some basic steps to take, and questions to ask, when bringing these solutions into your business.

Assess your organization's overall understanding of cloud computing.

- Discuss functionality and risks.
- Assess current policies and operating practices.

Ask the basics first: Why cloud computing?

- Understand business drivers propelling you towards cloud computing.
- Will sensitive data or business operations be hosted in the cloud? If so, why?
- Develop a preliminary risk outline to work and build on.

Outline a solid communication, awareness, and education plan.

- Develop custom sessions for executives, plus general content for all employees.
- Establish a "Cloud Board" of business and technical leaders to work through adoption strategies.
- Avoid organic growth models that are cumbersome to operate, scale, or secure.
- Measure consumption trends and determine risk tolerance.





The Demographic Shift: The Role of Collaboration and Social Networks

It's important to understand how prevalent—and valuable—social networking is to today's workforce. In particular, the “millennials”—people defined as 30 years old and younger, often referred to as “Generation Y”—may be spending less time using traditional business tools like email in favor of social networks. In its recent report on millennials' use of technology, management consulting, technology services and outsourcing company, Accenture, found that younger millennials spend slightly more than four hours a week on work-related email, compared to almost seven hours a week for older millennials. (While the study didn't address older workers, one can reasonably assume that workers in their 30s and 40s spend well over seven hours a week on email.) Instant messaging and texting, often via social networks, are replacing email as the favored communications tool for this generation.

Accenture also found that millennials make heavy use of social networking sites while on the job, whether their employers allow them to or not. According to the report, 45 percent of employed millennials use social networking sites when they're at work, but only 32 percent say that this use of social networks is supported by their IT departments.

A similar survey from Cisco also found that when workers want access to social networking technologies, they'll get it—even if it means circumventing corporate policy. The Cisco “Collaboration Nations” study surveyed IT decision-makers as

well as employees from organizations around the world. The study reported that 50 percent of end users admitted that they ignore company policy prohibiting use of social media tools at least once a week, and 27 percent said they change the settings on corporate devices to access prohibited applications.

At the same time, social networks like Facebook, first colonized by college students, are exploding in population and, not surprisingly, have become places to conduct business. Facebook has an audience that continues to grow at exponential rates: The site currently has

400 million active users, and that number is projected to grow to 1 billion by the end of 2010. Recognizing that the enterprise market is a lucrative one, social media companies are introducing tools specifically designed for this audience.

An instant-gratification workforce is emerging: Generation Y was raised with mobility at their fingertips, and IT needs to adapt its strategies accordingly (as online criminals will).

Social Media for Enterprises: Upside and Downside

Social media has become both a groundbreaking collaboration tool for enterprises moving toward the borderless network and a prime venue for the launch of attacks against individuals in the business. The Enterprise 2.0 trend may be cause for cheering from workers who embrace social networking tools, but it can lead to sleepless nights for executives who believe it opens the door to data loss, hacking, and reduced productivity.

Attempts to steal data launched via social media certainly pose enough of a threat to businesses—as any user of social networking sites has undoubtedly noticed, their friends and family members seem to spread malware inadvertently on a regular basis. And as data theft attempts launched via email become less successful, criminals continue to focus their attention on social media. According to data compiled by ScanSafe, now part of Cisco, less than 1 percent of malware encounters in enterprises in 2009 were driven by users clicking links in webmail. In the first quarter of 2010, this number

rose to 1.4 percent. This likely indicates that users are more cautious about responding to suspect email, and that email filters are doing their job.

Many enterprises, fearing the spread of malware and productivity losses, have clamped down on use of social media networks (as well as instant messaging) in the workplace, even though workers want access to them. According to ScanSafe data, 64 percent of ScanSafe's customer base blocks access to social networking sites for 50 percent or more of their staff.

It's 3 p.m.—What Are Your Employees Doing? Tending Their Virtual Fields

According to Cisco data examining how its customers' employees use Facebook, 7 percent of Facebook users spend an average of 68 minutes per day playing the popular interactive game FarmVille. Mafia Wars was the second most popular game; the 5 percent of employees who play Mafia Wars rack up 52 minutes of play daily. Café World, another popular game, is played by 4 percent of Facebook users for an average of 36 minutes per day. (See the chart below for statistics on other applications.)

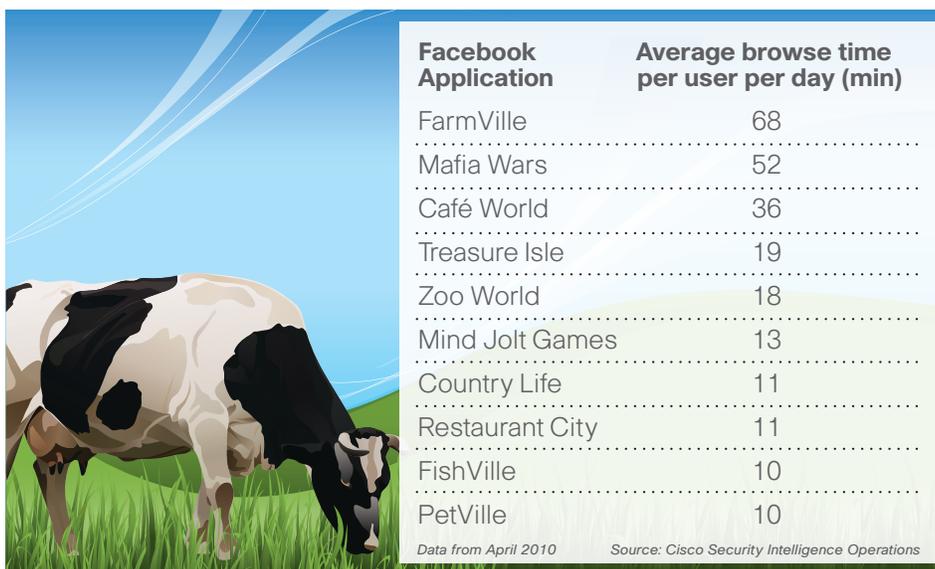
These numbers raise the question of whether enterprises should limit access to these interactive games, and by association, the social networking sites on which they operate.

While there may not be an immediate security risk in game-playing, it's safe to assume that online criminals are developing ways to deliver malware via popular applications. Heavy users love to search the web for cheats and tricks for better play, so they may fall victim to malware-laden links or spam messages offering such shortcuts.

However, if enterprises respond to this threat by banning all access to social networking sites, they may damage workers' ability to collaborate and communicate in a changing business environment. "Businesses must balance the need to provide access to collaboration tools with the need to manage enterprise security," says Christopher Burgess, senior security

advisor at Cisco. "The smartest solution is to create explicit policies governing the use of certain features, such as games, within social networking solutions. In addition, businesses need to be aware of exactly how and where workers are using such features."

How can enterprises minimize the threats that arise from the introduction of social media into the business? The best tactic is to develop a corporate social media handbook that includes information security policies and codes of conduct.



Interactive games have proven popular with Facebook users. Enterprises should set guidelines for where and how employees may access such games at work.

What's Disrupting the Enterprise? Social Media

Employees are pushing the boundaries of acceptable use of social networks and are slowly convincing even the most conservative enterprises that judicious use of these networks can benefit the business. But where, and how, are lines drawn?

For instance, enterprises may ban employees outright from using social media networks that offer messaging or chat, even though more and more business takes place via these messaging systems. If, for example, a company discovers that its customers and partners routinely use Facebook to stay in touch on projects, how does the business allow such access without giving workers free rein to distribute sensitive corporate information via these networks?

Businesses are slowly recognizing the power of social networking, but they haven't been quick to establish structures for its safe and secure use. A recent study sponsored by Cisco and conducted by leading business schools in Europe and the United States showed that organizations are lagging in governance and IT involvement when it comes to their social networking strategies:

- Social networking tools are making their way into many parts of organizations, such as human resources, marketing, and customer service. Small- and medium-sized businesses are using social networks for lead generation.

- Only one in seven of the companies participating in the study have established formal processes for adopting social networking tools for business purposes.
- Only one in five businesses said they had policies in place for the use of social networking tools.
- Only one in 10 survey respondents said their IT departments had direct involvement with social media initiatives.

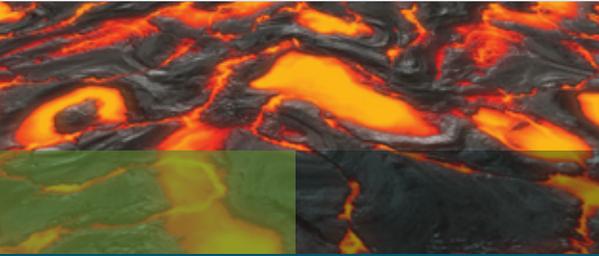
✔ ACTION ITEM:

Provide employees guidance.

Ideally, businesses would create policies that cover every possible incidence of social media use (and abuse). However, creating comprehensive policies may not be realistic, since the impact of social networking is still unfolding.

At minimum, enterprises should institute a process for allowing questions about social media usage to be directed to the correct decision-makers in the organization—in the absence of an environment that welcomes discussion, employees may make bad decisions that impact corporate security.





Worldwide Government Trends: The Impact on Business



As organizations adapt their security strategies to meet new and emerging technologic, economic, and demographic challenges, they also must acknowledge another powerful force: globalization. This, too, is having a significant impact on how and where business is done, and it's influencing security practices.

Multinational organizations, or those looking to do business on the global stage, must navigate the complexities and balance the demands of differing standards and attitudes toward security issues such as data loss protection and privacy in the various countries where they conduct—or want to conduct—business. If an enterprise adheres to certain standards in its primary markets of operation, will it be willing to make the effort to tighten the rules if it moves into a market where standards are more stringent—or conversely, loosen them, and perhaps put security and privacy at risk, in a market where standards are more lax?

Take, for example, the acts against major businesses, including Google, that are alleged to have occurred mid-to-late last year. These actions, dubbed “Operation Aurora,” involved a botnet that compromised computers in an effort to steal corporate information and break into email accounts. Google reported theft

of its intellectual property and also said that Gmail accounts of prominent human rights activists had been attacked.

Google executives, also unhappy about China's ongoing censorship of search engine results, announced in March that they would begin redirecting Google users in China to uncensored search results using servers based in Hong Kong. As of mid-March, business repercussions of this decision were becoming evident: According to *The New York Times*, China Mobile, the company's biggest cellular company, would cancel a promotional deal placing a link to Google on its mobile Internet homepage. But the story has no clear ending—as this report went to press, Google said it was responding to threats from the Chinese government to revoke its operating license by changing (yet again) its approach to dealing with Chinese users.

Multiple Governments, Multiple Stances on Security

The differing standards among countries for maintaining the security of corporate data can be a source of frustration for businesses. Many countries are concerned with the effects on economic and national security arising from cybersecurity. Policymakers across the globe are trying to find approaches to security that both protect the assets of their citizens and function globally. This conversation will continue for some time, but enterprises should be aware that policymakers may issue conflicting requirements. Businesses should recognize this challenge and work globally to ensure consistent policies that protect and encourage innovation.

To the extent that enterprises are subject to nonstandard requests from the governments of countries with which they do business—like the request to use nonstandard encryption—organizations must decide if they will consent to these demands, and how they will protect their customers and employees from possible data breaches if they do so.

There are signs that governments may band together to add some cohesion to the varying security and privacy standards across borders—especially since the rise of country-specific security requirements threatens to fragment the global interoperability of the Internet. Common Criteria is a set of security standards that many countries and enterprises (including Cisco) have adopted to enforce security standards while striving to attain global interoperability. And in March, British lawmakers called for a Europe-wide approach to cybersecurity instead of ad hoc fixes country by country, as “the collapse in cybersystems in one country can overlap in others.”¹⁰

Global Security Guidelines: Should Business Become a Player?

It’s not only the U.S. government that is prioritizing cybersecurity. Governments, aware of the national security implications of critical infrastructure assets owned and operated by the private sector, are beginning to encourage more private-public sector security cooperation.

Private entity assistance is particularly valuable for organizations that are working to establish standards across borders. For instance, global nonprofit Internet Corporation for Assigned Names and Numbers (ICANN), which assigns the Internet’s domain names and IP addresses, has a Government Advisory Committee

consisting of local government representatives, as well as task forces comprised of relevant businesses, such as networking companies and equipment vendors.

The U.S. federal government is reaching out to the private sector to develop standards as well. In March, U.S. Chief Technology Officer Aneesh Chopra emphasized the need for collaboration between the government and private sector in a blog post on the Office of Science and Technology website. He wrote, “It is more important than ever that federal agencies work effectively with the private sector to ensure that meaningful standards can be in place to meet urgent national needs.” He added, “The right starting point is to ensure that federal agencies work closely and effectively together to define their standards needs, define their approach to working with industry and standards organizations, and support their meaningful adoption by markets.”¹¹

One issue to consider when implementing these partnerships: If an enterprise partners with one government, it may lose out on business from another country because they may believe the business would relay sensitive information between countries. In addition, a business’s own customers may suspect that the enterprise is getting too close for comfort with government officials, and may be sharing private customer data. These perceptions need to be managed directly and proactively if businesses intend to proceed with certain types of government partnerships.

There’s another twist to the security partnership angle: the idea of enterprises creating information sharing committees (ISACs) to share more information about the threats they encounter. This is not a new concept, but it’s one that should take on more urgency as threats increase. After all, the miscreant community is collaborating. According to the *Dark Reading* security news web portal, the Bay Area CSO Council, whose members comprise chief information and security

officers from leading San Francisco and Silicon Valley area businesses (including Cisco), is already stepping up this information sharing.

“When an advanced persistent threat (APT) attack occurs, many members are on the phone with one another three times a week rather than for just their regular monthly teleconferences,” reports *Dark Reading*. The council is also creating an online portal where members can record data about attacks and threats, hopefully correlating information and sharing advice on defensive tactics.

U.S. Government Update

Over the past year and a half, businesses of all types have been monitoring the Obama administration’s progress on strengthening U.S. national cybersecurity, wondering how they might benefit—or perhaps be affected adversely—by new rules and expectations set by the government. They also wonder what they may be asked to change or provide to help the president meet his ambitious goals.

There has been concrete progress on several fronts since President Barack Obama unveiled his cybersecurity plan shortly after taking office in 2008. The administration remains focused on cybersecurity issues, and it can be said that cyberdefense in the U.S. government, and in the country at large, is improving. There is increasing transparency, for example, with more reporting of threats, intrusions, and hacking incidents related to unclassified systems. Just as in the private sector, however, the threat of cyberattack remains a significant issue for government.

Director of National Intelligence Dennis Blair, who stepped down from his post in mid-May, highlighted the issue for the U.S. Congress earlier this year, indicating that the nation’s computer networks remain vulnerable to intrusion or disruption, and that criminals are stealing information from the government and private sector every day. He told lawmakers, “Malicious

¹⁰ “Europe ‘vulnerable to cyberattack,’” by Bobbie Johnson, Guardian.co.uk, March 18, 2010, www.guardian.co.uk/technology/2010/mar/18/europe-vulnerable-to-cyberattack.

¹¹ “Providing Leadership on Standards to Address National Challenges,” by Aneesh Chopra, Office of Science and Technology Policy blog post, March 24, 2010, www.whitehouse.gov/blog/2010/03/24/providing-leadership-standards-address-national-challenges.

cyberactivity is occurring on an unprecedented scale with extraordinary sophistication.” Blair also referenced the Operation Aurora incident in 2009 (see page 13) as a “wake-up call” for U.S. officials. He emphasized that “cyberspace [cannot be protected] without a coordinated and collaborative effort that incorporates both the U.S. private sector and...international partners.”¹²

While the Obama Administration’s efforts to create a national cybersecurity plan have been considerable, continued development has slowed as debate continues over authorities, roles, and responsibilities between the public and private sectors.

There has been increasing dialogue between private industry and the government about improving U.S. cybersecurity—both domestically and globally. Cybersecurity coordinator Howard Schmidt wrote on the White House website in March 2010: “In order to be successful against today’s cybersecurity threats, we must continue to seek out innovative new partnerships—not only within government, but also among industry, government, and the American public.” President Obama appointed Schmidt as the first White House cybersecurity coordinator in December 2009. His choice of Schmidt, who has 40 years of experience in government, business, and law enforcement, was well received by cybersecurity professionals.

Another high-profile initiative by the Obama administration starting to take shape is the U.S. Cyber Command (U.S. CYBERCOM). Part of the Department of Defense, CYBERCOM’s purpose is to protect military networks against malicious cyberattacks. President Obama’s nominee for the first U.S. CYBERCOM commander, Army General Keith B. Alexander—who also leads the U.S. National Security Agency (NSA)—was appointed in late May

2010 and given a fourth star. His appointment officially established the initial operating capability for the new command, which should be fully operational by the end of this year. About 2500 personnel are expected to be hired and positioned, primarily at Ft. Meade, Maryland, where U.S. CYBERCOM is located and the NSA is based.

One concern expressed when General Alexander was nominated to lead CYBERCOM was that he is also the director of the NSA, and would therefore assume a “triple-hatted” role because he also leads the Central Security Service. However, General Alexander told the Senate Armed Services Committee in April 2010 that if confirmed for the top role at CYBERCOM, he would not try to “militarize cyberspace” and would focus on safeguarding the integrity of the military’s critical information systems. In addition, he pledged that he would work to protect the privacy rights of Americans.¹³

Meanwhile, cybersecurity-related hiring at the Department of Homeland Security (DHS) has been slowly increasing, as last fiscal year it was given more than US\$385 million for new personnel. The DHS has been working to locate available talent and has been aggressively seeking candidates from outside the government because there simply aren’t any existing personnel to spare—and getting clearance for those they do hire is a lengthy process (as long as 12–18 months for certain positions). The DHS is also exploring hiring existing contractors for full-time cybersecurity roles.

Privacy Issues Moving to the Forefront

In the year ahead, expect the discussion around civil liberties and privacy issues to intensify in the United States, in particular, as the country takes a more defensive posture with its cybersecurity. Why should the private sector pay attention? Because they may end up doing the “heavy lifting” on these issues, with the U.S. Congress and the American public asking what companies are doing to help protect against the erosion of citizens’ privacy, while also doing their part to help strengthen national cybersecurity.

Meanwhile, businesses have been airing their concerns to the government about privacy, but from a different angle—specifically, how disclosure about an attack can undermine their competitive edge and damage their reputation. At the RSA Conference in March 2010, U.S. Federal Bureau of Investigation (FBI) Director Robert Mueller pledged “minimal disruption to business with protective orders and increased privacy for U.S. corporations who suffered data breaches, in order to avoid loss of reputation and brand—despite the momentum of federal and state data breach disclosure laws.”¹⁴

He said, “Notifying the authorities may harm your competitive position. We will minimize the disruption into your business. We [will] work together to limit the breadth and scope of [the] attack. For every investigation in the news, there are hundreds that will never make the headlines. Disclosure is the exception, not the rule.”¹⁵

“The government is not going to secure the private sector. [But] we are making sure our private sector partners have more security as part of what we are doing.”

—Howard Schmidt, U.S. cybersecurity coordinator

12 “Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence,” testimony to the U.S. Congress by Dennis C. Blair, Director of National Intelligence, February 2, 2010, www.dni.gov/testimonies/20100202_testimony.pdf.

13 “NSA Director Says Cyber Command Not Trying to Militarize Cyberspace,” by Brian Prince, eWeek.com, April 15, 2010, www.eweek.com/c/a/Security/NSA-Director-Cyber-Command-Not-Trying-to-Militarize-Cyberspace-602442/.

14 “RSA: FBI Director Calls for Action Against Cyber Threat,” by Stefanie Hoffman, ChannelWeb, March 5, 2010: www.crn.com/security/223101709jsessionid=OXDPJJJQFNIOVQE1GHRSKH4ATMY32JVN.

15 Ibid.



Taking Action to Reduce Innovation Gaps



To date, governments and law enforcement worldwide have been making slow progress on improving cybersecurity and increasing the fight against cybercrime. Meanwhile, cybercrime continues to grow: Last year, in the United States, the total loss linked to online fraud was US\$559.7 million—up from US\$265 million in 2008.¹⁶

Why are cybercriminals so successful? In their shadow economy, just as in the commercial business world, those who move fastest and use technological innovation to their advantage succeed or displace the competition (see *Criminals Now Protecting Their Intellectual Property*, page 17). It's simple Darwinism: The most agile survive.

For all the innovation in adopting technology in the private sector, in some areas criminals move even faster. While many legitimate businesses are still weighing the benefits of embracing social networking and peer-to-peer technologies,

cybercriminals were early adopters of these innovations and are using them not only to commit crime, but to enhance their communication, refine and promote their areas of expertise, and speed their transactions with each other.

In Russia, for instance, social networks were used to create an online marketplace for stolen credit cards. This has allowed the “sellers” to specialize in areas such as acquisition, while the “buyers” focus their efforts in exploitation. In addition, terrorists worldwide are using social networks to organize, recruit, and learn; military analysts call this “open-source warfare.”

There is also another type of “innovation gap”: the gap between how quickly criminals can innovate to exploit vulnerabilities and the speed by which businesses can innovate to protect their systems. It is critical to recognize just how rapid the cybercriminals’ development and deployment cycle is. They don’t have to answer to shareholders, laws, or regulations. In fact, a major part of their role is to find ways around established systems, policies, and protective controls. There is no need to spend hours in the research and development phase making sure their results are proof-positive. If something works, they will run with it.

¹⁶ “IC3 2009 Annual Report on Internet Crime Released,” media release, March 12, 2010, The Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center (NW3C), www.ic3.gov/media/2010/100312.aspx.

Malicious technology often can be deployed in hardware or software products as soon as it's developed. (Consider how many times we have witnessed the compromise of a product on the day it is released.) For the software industry, specifically, closing the innovation gap means making sure security is factored into the development cycle, with every effort made to detect and eliminate vulnerabilities in products before they are released so they are as secure as possible when introduced to the market.

For enterprises, an important first step toward bridging the innovation gap is to harden their security through a renewed focus on security basics, says John Stewart, vice president and chief security officer of Cisco. "One reason why many hacking scenarios succeed is because a critical element of a network or an individual within a network is trivially compromised," he explains. "Part of the 'innovation gap' is that organizations are just fighting the latest threats—focusing on whatever is the shiniest object in the security threat

landscape—instead of staying on top of old and current problems that remain popular paths of attack for criminals."

To reduce the innovation gap, Stewart recommends that enterprises:

- Move faster to implement new technology when needed instead of hanging on to outdated technology, hardware, and software, simply because it's already in place.
- Measure the efficacy of security controls: not only the technology, but the combination of people, processes, and technology in the organization.

In addition, businesses should take the time to build a working relationship with law enforcement, such as nonprofit organization InfraGard (www.infragard.net) in the United States, a private-public partnership with the U.S. FBI, and in the United Kingdom, the Police Central e-Crime Unit of the Metropolitan Police (www.met.police.uk/pceu/). Enterprises need a "go-to" team in the event of a cybersecurity incident, and they should

know exactly what type of information to provide to law enforcement to help them track down and prosecute cybercriminals.

While many leading companies are taking a more proactive approach to security, others continue to view it as an afterthought. Too often, C-level executives are allowed to label security as "IT's problem."

But in the enterprise, security is everyone's problem. If business organizations don't embrace that mindset, the innovation gap can never be bridged. "Malicious actors only need to get it right once. But we have to be right all of the time," says Stewart.

Criminals Now Protecting *Their* "Intellectual Property"

However cutting-edge and entrepreneurial you believe your business is in terms of technology and security, remember one thing: The criminals who prey on business online are trying to always be a few steps ahead of you. Witness the trend of creators of malicious software placing tough anti-piracy protections on their creations, in a bid to keep other criminals from stealing their intellectual property.

The latest version of the builder kit for the Zeus banking Trojan, which has long been a threat to financial institutions and delivers lucrative personal information back to a botnet command-and-control server, includes the type of copy protection one would normally find on a sophisticated piece of enterprise software. The creators of Zeus have added a hardware-based licensing system to the Trojan builder kit, which only allows the kit to be copied on a single computer.

The creators of a competing malware kit, SpyEye, which appears to be trying to gain market share from Zeus, have also decided to protect their technology. "Not to be outdone [by Zeus], the SpyEye author now claims his malware builder

also includes a hardware lock, using VMProtect, a Russian commercial software protection package," reports the Krebs On Security blog.

It's sobering news that criminals are quickly meeting and even exceeding the safeguards that legitimate enterprises build into their products—yet another sign that the sophistication and business acumen of online criminals knows no bounds. Also of concern is the fact that protected malware code and software can be harder to reverse-engineer, and therefore, more challenging for enterprises and their security vendors to develop ways to halt it.



The Spread of IPv6 and Domain Name System Security



Thanks to its explosive growth, the Internet is running out of IP addresses that were established under the IPv4 protocol, created 35 years ago. (IP addresses have traditionally been represented by four sets of numbers, such as 192.168.1.1.) Current predictions call for IPv4 addresses to be depleted by 2011 or 2012. The solution is the new IPv6 protocol, which will allow for substantially more IP addresses, thus providing trillions upon trillions of new addresses, dramatically increasing the ability to keep up with the Internet's growth.

Even though IPv6 has not been widely deployed, there has been much security testing and development of mechanisms to secure the protocol. Many commercial security testing tools have been updated to support the IPv6 protocol; many others have it on their road maps. Various security concerns around IPv6 have already been identified, such as insecure neighbor discovery, tunneling, and auto-configuration. Early security research has led to the development of the RFC 3971 Secure Neighbor Discovery Protocol (SEND) and RFC 3972 Cryptographically Generated Addresses (CGAs), which help mitigate the weaknesses with the default neighbor discovery process and are not vulnerable to the same attacks. One drawback, however, is that not all devices support these new standards.

In mid-2009, Cisco Distinguished System Engineer Eric Vyncke told *Network World* that IPv6's auto-configuration capabilities can allow criminals to establish rogue network devices that masquerade as IPv6 routers. An IPv6-capable device can automatically configure itself with a local IPv6 address without being specifically configured for IPv6; this can open up a new attack vector unbeknownst to the user.

In addition, the process of shifting to the IPv6 standard, including the development and deployment of IPv6-ready security devices and networking equipment, may expose enterprises to exploits because security vulnerability testing is only in the beginning stages.

Combating the threat posed by IPv6 may mean simply raising awareness among IT staff that the process of switching to the standard should not be done without thorough testing and researching of potential vulnerabilities. No business should assume that because the new standard is solving one problem, it isn't creating others.

Like IPv6, Domain Name System Security (DNSSEC) promises to make life better for individuals who, and businesses that, rely on the Internet. But it also may raise unrealistic expectations that it can solve all the security "pain points" that plague the online world. DNSSEC reduces the chances for criminals to launch attacks via DNS cache poisoning (a type of "man-in-the-middle" attack), in which users are redirected from legitimate to malicious websites without their knowledge.

DNSSEC uses public key cryptography to create digital signatures that assure web users they have been directed to the correct IP address that corresponds to the web address they typed into their browser. Enterprises that embrace use of DNSSEC should be aware that while the standard promises to thwart a troublesome type of online attack, it will not solve all security challenges.

▲ RISK ALERT: A "Perfect Storm" of Technological Change

IPv4 address exhaustion and the move to IPv6, the need to implement DNSSEC, and the switch from 2-byte to 4-byte Autonomous System Numbers (ASNs), which marks a change to the Internet's inter-domain routing structure, will ultimately change the way the Internet functions. Any one of these changes represents a significant architectural and operational challenge for network operators. Together, they create a "perfect storm"¹⁷—described as "the greatest and potentially most disruptive set of circumstances in the history of the Internet, given its growth in importance to worldwide communications and commerce."¹⁸

Of course, this means that enterprises are at risk as well. The question: Is your enterprise prepared for the arrival of these "multiple, simultaneous, and large-scale changes"?¹⁹ The storm is approaching fast—but organizations have known for years that it was coming. Therefore, your security team already

¹⁷ *Worldwide Infrastructure Security Report*, Arbor Networks, January 19, 2010, www.arbornetworks.com/report.

¹⁸ "Perfect Storm Threatens Telecom Networks," by Carol Wilson, *Light Reading*, January 19, 2010.

¹⁹ *Ibid.*

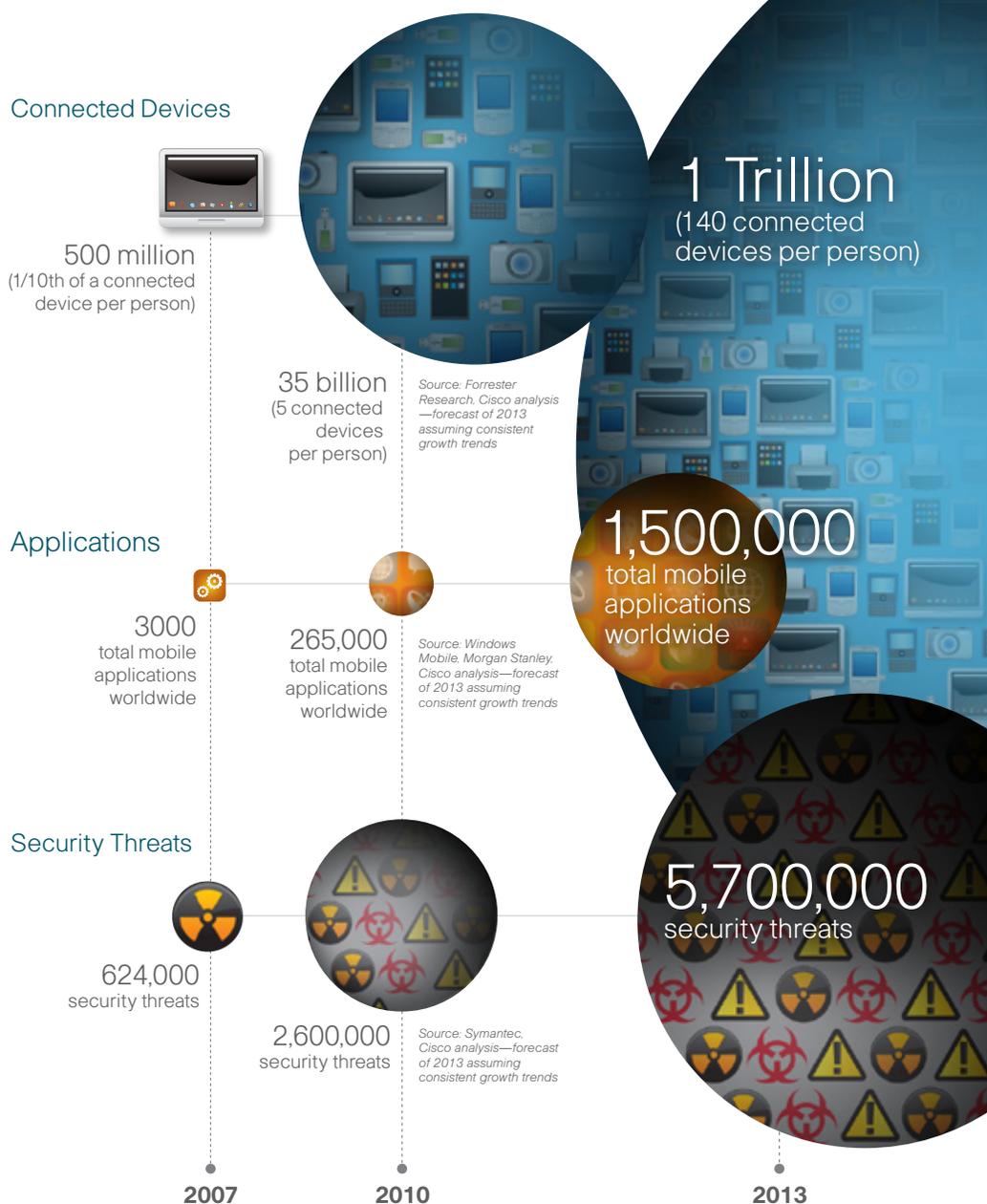
Explosive Growth in Connected Devices and Applications—Along with New Threats

The dramatic technology and security changes impacting enterprises are accelerated by the projected growth in usage of mobile devices and applications. Unfortunately, criminals don't intend to allow their activities to lag behind this growth—security threats are expected to multiply in tandem with the adoption of these devices and applications.

As seen in the chart below, as of 2010, about five connected devices per person are in operation worldwide—but that number will seem puny in 2013, when projections call for a whopping 140 devices per person to be in operation globally. At the same time, security threats will be on a similarly dramatic trajectory: from 2.6 million identified threats this year, to 5.7 million in 2013.

should be carefully planning for these changes and making necessary updates so they can help minimize the organization's security exposure and ensure the network infrastructure, from routers to firewalls to switches to software, is protected as the transition to each new service occurs.

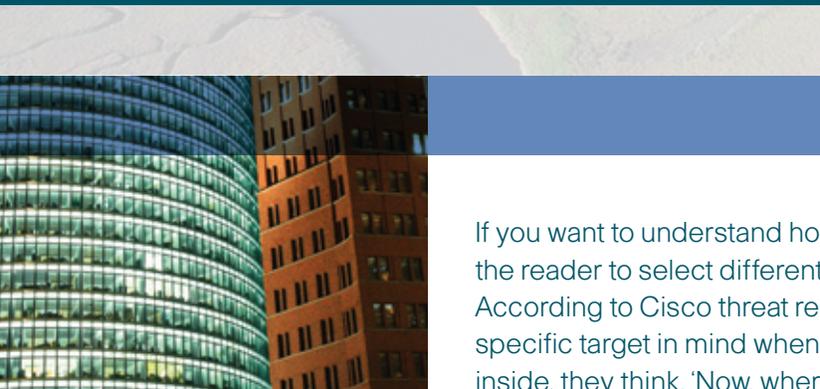
Expect to see many businesses preparing for the storm in the coming year. They will likely need to expend a great deal of time, money, and resources on adapting to these significant changes, which are inconveniently culminating post-recession, when IT resources are already limited at many organizations. U.S. government organizations are likely to be particularly preoccupied with getting up to speed, as many failed to comply with the December 31, 2009, deadline set by the U.S. Office of Management and Budget to deploy new authentication mechanisms (for example, digital signatures for DNSSEC) on their websites that would help prevent hackers from hijacking web traffic and redirecting it to bogus sites.²⁰



²⁰ "80% of government Web sites miss DNS security deadline," by Carolyn Duffy Marsan, NetworkWorld.com, January 21, 2010, <https://www.networkworld.com/news/2010/012010-dns-security-deadline-missed.html?page=1>.



Insight from the Security Researchers: Hackers Are Choosing Their Own Adventure



If you want to understand how today's hackers operate, think of a book that allows the reader to select different storyline options to pursue at the end of each chapter. According to Cisco threat research manager, Scott Olechowski: "They have a specific target in mind when they break through the firewall. But once they are inside, they think, 'Now, where else can I go from here?'"

**"Why do hackers succeed?
They're lucky, they're patient,
and they're brilliant. They're
also better funded than you."**

—John Stewart, vice president and
chief security officer, Cisco

Olechowski also emphasizes that while hackers may decide to explore at random inside a network, their end goal is constant: to collect as much valuable information as possible, for as long as possible (see *Advanced Persistent Threats*, page 22).

"It's all about building a path in the network that you can travel many times until you have all that you want, or you are discovered—if you ever are," he says.

Today's hackers are usually doing a job for someone else—and their contact, in turn, may be working for someone else, and so on. (This chain can lead to other companies or even governments, not just an individual or criminal organization.) Good information always has "street value," and an impressive amount of money is likely to change hands between those who steal data and those who want it—from thousands to millions, depending on what the information is, how much there is, and who is funding the

operation. This is why the theft of intellectual property is now garnering more attention than ever from industry: It has become a real threat to businesses' continued ability to compete and conduct commerce.

ScanSafe has been tracking malware encounters in highly sensitive industries for two years, and its research has revealed—perhaps, not surprisingly—that companies in the energy and oil, pharmaceutical and chemical, government, and banking and finance sectors are being targeted by hackers and other cybercriminals seeking intellectual and corporate assets and government intelligence. Targets for attack include executives and other key employees who have direct access to this type of information (see *The Downside of Being a VIP (or Just Working for One)*, page 22).

Kurt Grutzmacher, network consulting engineer in the Cisco Advanced Services Security Posture Assessment team, knows well what today's hackers are after—and how they get to it. Cisco customers hire the Security Posture Assessment team to impersonate attackers and expose vulnerabilities through penetration testing. "Using common exploits, we try to crack into the customer's network and poke around to see how deep we can go and what we can find, from personally identifiable information (PII) and financial data to intellectual property, including source code," explains Grutzmacher.

The Security Posture Assessment team looks for common security soft spots, such as unpatched servers and easily guessable account credentials. "If we are coming into and then 'sitting' in the network, we look specifically for the weaknesses in account management, such as easy-to-crack passwords and IDs, unprotected databases, and web applications that IT might not be aware of or that have known weaknesses," continues Grutzmacher. "Organizations are usually quite surprised by how much sensitive data we can collect that they were convinced was safe—or they thought wouldn't be of interest to a hacker."

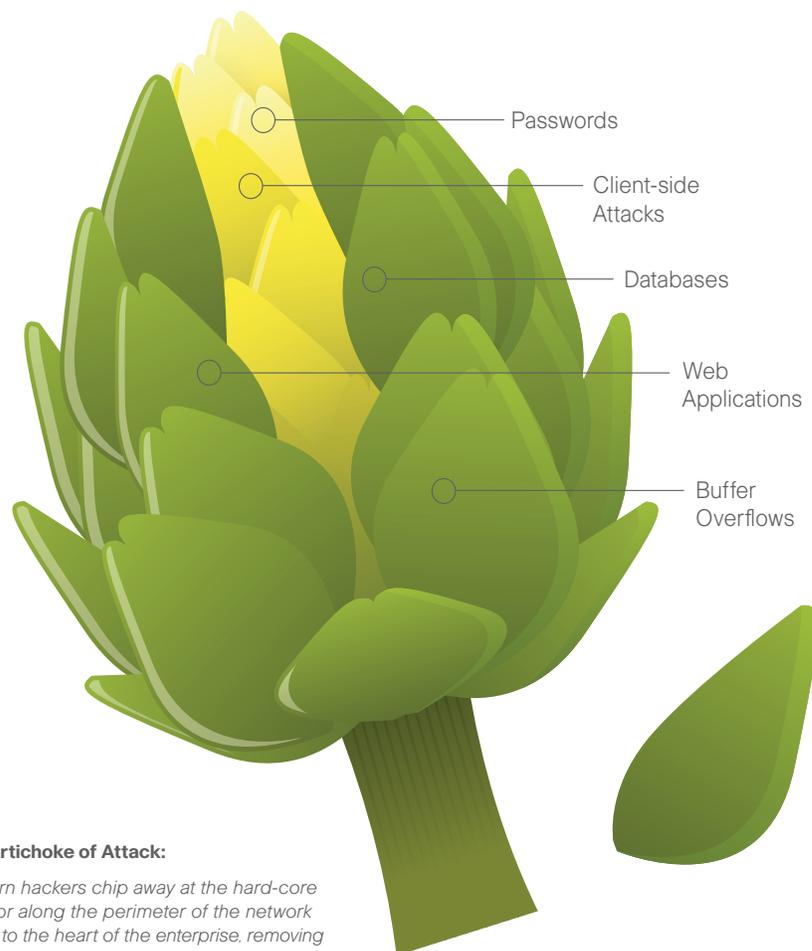
Weak credentials are a boon to hackers, who will "ride" the compromised credentials as far as they will take them, deeper into areas of the enterprise where sensitive data resides, often with limited or no security measures to protect it. But it's not always data that's the prize. Hackers sometimes gain control of large parts of a computing environment by seizing administrative access and taking over an organization's network devices, Windows domain or UNIX databases. There, they'll wait and capture the day-to-day operations of the business, including email communications, instant messages, and websites visited by employees.

Grutzmacher calls the modern hacker's approach to breaking into a network and stealing data the "Artichoke of Attack": The hacker chips away at the security armor along the perimeter to get to the "heart" of the enterprise. While Internet-facing systems are usually very well protected and boundary protections are typically solid, persistent hackers—aided by a mix of skill and luck—do eventually find a gap in that hard-core exterior through which they can enter and go where they please.

"You used to hear about hackers having to peel away at the network's 'onion layers,' but in the borderless environment, that analogy does not apply," Grutzmacher says. "Hackers don't have to peel away the layers—they only need to remove certain pieces. The bonus is that each little part is tasty. And leaf after leaf, it all leads the hacker to something even more tasty."

"You used to hear about hackers having to peel away at the network's 'onion layers,' but in the borderless environment, that analogy does not apply."

—Kurt Grutzmacher, network consulting engineer, Cisco



The Artichoke of Attack:

Modern hackers chip away at the hard-core exterior along the perimeter of the network to get to the heart of the enterprise, removing certain "leaves" to reveal sensitive data that is either unprotected, or secured by weak defenses, such as easy-to-crack passwords and IDs.

▲ RISK ALERT:

Advanced Persistent Threats

Like the so-called “sleeper cells” that plague those who fight terrorism, persistent threats present a danger to enterprises that have not implemented ways to identify and stop these security challenges. Instead of constant, “noisy” attempts, persistent threats favor a “low-and-slow” approach. This type of exploit may center on malware that, once lodged in the network, communicates only infrequently with its command-and-control networks to evade detection, or uses social networks and other hard-to-filter means to communicate inconspicuously.

“Advanced persistent threats” or APTs are launched by skilled attackers whose goal is to cause severe economic disruption to the business and to gather intelligence in a targeted manner. For instance, they may seek anything from competitive bids to natural resource contracts to engineering documents. (Operation Aurora, discussed on page 13, is an example of an APT.)

Because these threats are designed to remain under the security-detection radar, the intruders intend to return repeatedly to a specific target, stealing more information. These attacks are also adaptive, meaning they will change tactics based on your defenses. This is not a “smash-and-grab” crime—it is a well-planned, long-term scheme to separate a business from its money or intellectual property, or to gain competitive advantage.

The perpetrators of an APT launch their intrusion with the goal of stealing information—perhaps intending to sell it to a competitor. And when they want to gather more data, they don’t need to breach network defenses again, since they’re already inside the network and presumably undetected. “Advanced persistent threats reinforce the idea that the current cybercrime landscape is driven by business-minded, well-organized crime syndicates,” warns Henry Stern, senior security researcher at Cisco.

How can enterprises combat such sophisticated and potentially devastating threats? Not surprisingly, detection of APTs is difficult once they have established a presence in your network. “When a hacker is inside the network, it really becomes a game of hide-and-seek,” notes Kurt Grutzmacher of the Cisco Advanced Services Security Posture Assessment team. Most corporate security systems are concentrated on inbound traffic only, which means that if an APT manages to work its way past the perimeter defenses, it may not be detected again.

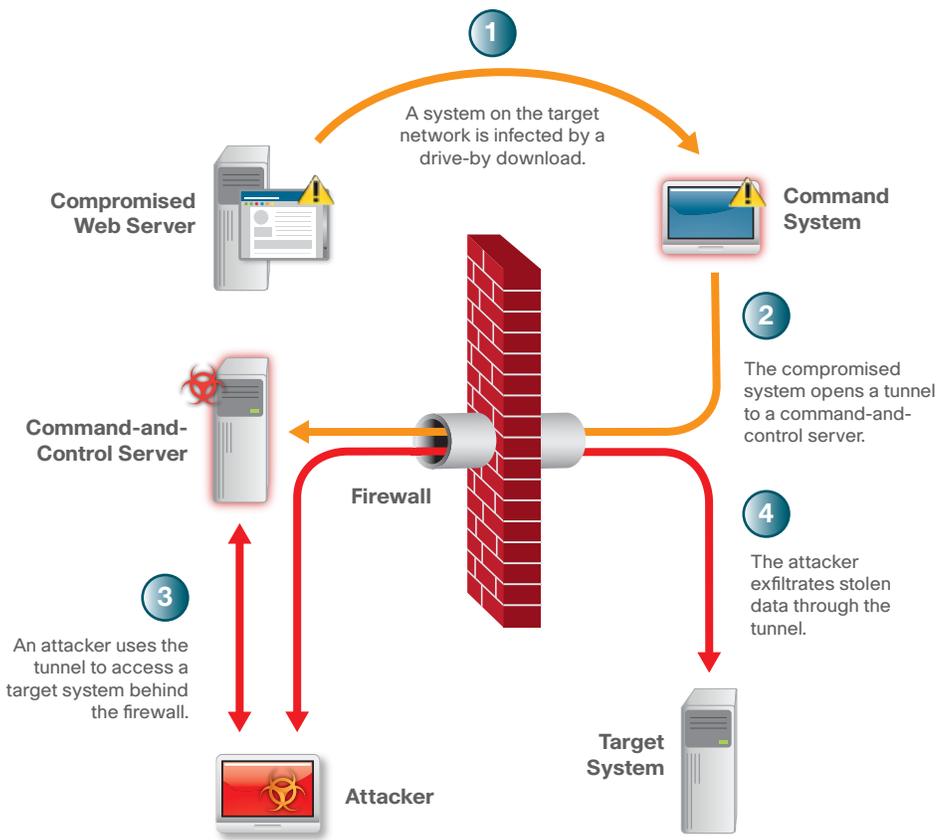
The best defense against APTs is to prevent infection to begin with, relying on user education and network- and host-based defenses. However, enterprises must acknowledge the risk of APTs, and have the ability to detect them if an infection occurs. Enterprises often have the tools necessary to detect APTs and stop data exfiltration, but they lack awareness of this threat’s existence, and therefore do not focus attention on them.

Enterprises’ tools to detect APT infections on corporate networks include network monitoring, egress filtering, and data loss systems in conjunction with baselining “normal” network usage, outbound traffic log analysis, and data on the command-and-control nodes used as upload points for data theft. These tools, used in combination, are key to detection of the APT threat.

▲ RISK ALERT:

The Downside of Being a VIP (or Just Working for One)

Not all vulnerabilities lie in an enterprise’s hardware and software. Highly visible executives are walking and talking vulnerabilities because they are privy to sensitive business information. So, too, are other employees who are authorized to access financial information, intellectual property, and other highly sensitive data—in fact, such workers are potentially more vulnerable and more frequently targeted than top executives. They are prime targets because the payoffs can be great. Instead of sending a phishing email to every employee in an attempt to steal network login info—a scattershot



Advanced Persistent Threats (APTs) remain under the security-detection radar, and thus are difficult to detect and eliminate.

Small Targets, Big Rewards



Small towns, cities, counties, and municipalities—and small banks and credit unions—have become popular targets for looters of online bank accounts. The theft of “modest” sums ranging from US\$10,000 to US\$500,000—or more—can quickly grow the balance sheets of successful criminals.

In one recent case in the United States, thieves targeted the assistant of the administrator of a small town near Chicago. When the assistant attempted to log on to the town’s local bank account, she was redirected to a page informing her the bank’s website was experiencing technical difficulties—a delay tactic that allowed the criminals

enough time to create their own interactive session with the account.²¹ The assistant was even provided a fake phone number for customer service, which she later called and found to be a residential number.

By the next day, the thieves had transferred US\$70,000 out of the town’s bank account. Fortunately, the bank (after notifying town staff of the previous transfers and learning they were the work of thieves) was able to halt one fraudulent wire transfer of US\$30,000. This prevented the total amount stolen from the small Illinois town of 10,000 from reaching six figures.

21 “Computer Crooks Steal \$100,000 from Ill. Town,” by Brian Krebs, Krebs on Security blog, April 6, 2010, <http://krebsonsecurity.com/2010/04/computer-crooks-steal-100000-from-ill-town/>.

approach that is easier to detect and block—criminals prefer to hone in on someone with access, because that individual can lead them directly to what they want.

Aside from technological approaches to preventing phishing messages (such as reputation management) from reaching executives and other VIPs, prevention comes from a heightened awareness of the danger of exposing insider data unwittingly to the public. Cybercriminals have become adept at creating very convincing phishing emails designed for so-called “whaling,” because there is so much detailed information about executives available in the public domain. Even a few indiscreet Twitter or Facebook posts by a highly placed executive can provide enough hints for criminals trying to decide if your business has information someone else will pay for. Criminals are also skilled at piecing together seemingly innocent bits of data to crack passwords and hack into email accounts.

“If a stranger came up to you on the street, would you give him your name, Social Security number, and email address? Probably not,” wrote *New York Times* reporter Steve Lohr in March of this year. Yet, wrote Lohr, everyone from CEOs to teenagers has become conditioned to the idea of sharing all sorts of private and professional information. Last year, reported the *Times*, researchers from Carnegie Mellon University demonstrated that, using publicly available information from several sources such as social networks, they could reliably predict the Social Security numbers of nearly 5 million Americans in fewer than 1000 attempts.

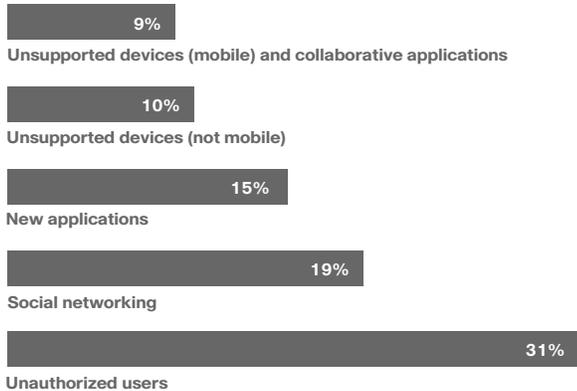
Threats directed to top executives are not always delivered by email, however—devices also can become a channel to be exploited. Executives are quite often the employees pushing hardest to have the devices they want, such as trendy smartphones, allowed into the enterprise. Many don’t even ask IT for permission when they access corporate assets with unsupported devices, creating obvious

data and network security risks. Some criminals, recognizing this, aim Trojans directly at devices used by executives, such as smartphones—or even a device far less complicated, like a USB drive. Once the device is connected to a laptop or desktop computer, the Trojan can launch and seek access to sensitive corporate data.

The mobility of today’s executives compounds privacy and security headaches: The more time on the road, the more opportunities for laptops and mobile devices to be stolen or lost. The C-suite and other VIPs in the organization need the same training that all workers receive—and perhaps, even a bit more. They must understand the risks to the enterprise due to their everyday use of technology, from slipping sensitive competitive information into a seemingly innocuous discussion via social networks to leaving their laptop in an airport terminal to using a malware-carrying flash drive they picked up at a recent trade show.

What Keeps Your IT Security Team Awake at Night?

New research data from Cisco reveals what IT security professionals—those responsible for setting, maintaining, and communicating corporate security policies—believe are some of the most worrisome security risks to the enterprise. The top five issues, according to a global multiple choice survey of IT security decision-makers from organizations in industries ranging from education to government to finance to transportation, are depicted in the graphic below.*



*More than one answer allowed.

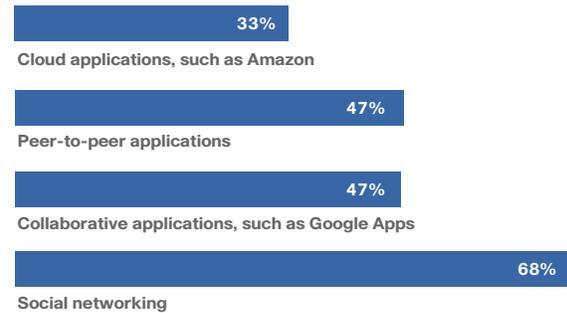
“The top five concerns of IT security professionals worldwide clearly align with the technologic, economic, and demographic forces of change that are having an impact on businesses,” notes Ambika Gadre, senior director of security product marketing, at Cisco. “IT teams are concerned about unauthorized users gaining access to the network and sensitive corporate data by taking advantage of two areas where the enterprise increasingly lacks visibility and control: unsupported mobile devices and Web 2.0 applications.”

Restrictive Policies Common Worldwide

More than 40 percent of all survey respondents said they have determined their employees are using unsupported network devices, and 80 percent said they restrict what employees bring onto the network (with organizations in the United States and Germany being the most restrictive). And four in 10 IT security professionals report their company has lost information due to unsupported network devices.

However, nearly the same number (39 percent) of respondents said their organizations are “very likely” to allow employees’ personal devices on the network in the next 12 months—with China (59 percent) and India (54 percent) being most receptive to that change, even though survey results for those countries show they had the highest number of data losses or security breaches due to such devices. Overall, only 7 percent of organizations worldwide already allow the use of personal devices on the enterprise network, according to the survey.

Meanwhile, 56 percent of all respondents noted that their employees are using unsupported applications. The graphic below lists the types of unsupported applications that are most prevalent in the enterprise, according to the survey results.*



*More than one answer allowed.

Nearly half of respondents (48 percent) said their organization tracks application vulnerabilities through vendor notifications. More than half of all respondents said they conduct assessments of the security applications and operating systems that employees are using, the types of devices and nonsecurity applications they are running, and at what locations they are working.

Employee Training Central to Policy Enforcement

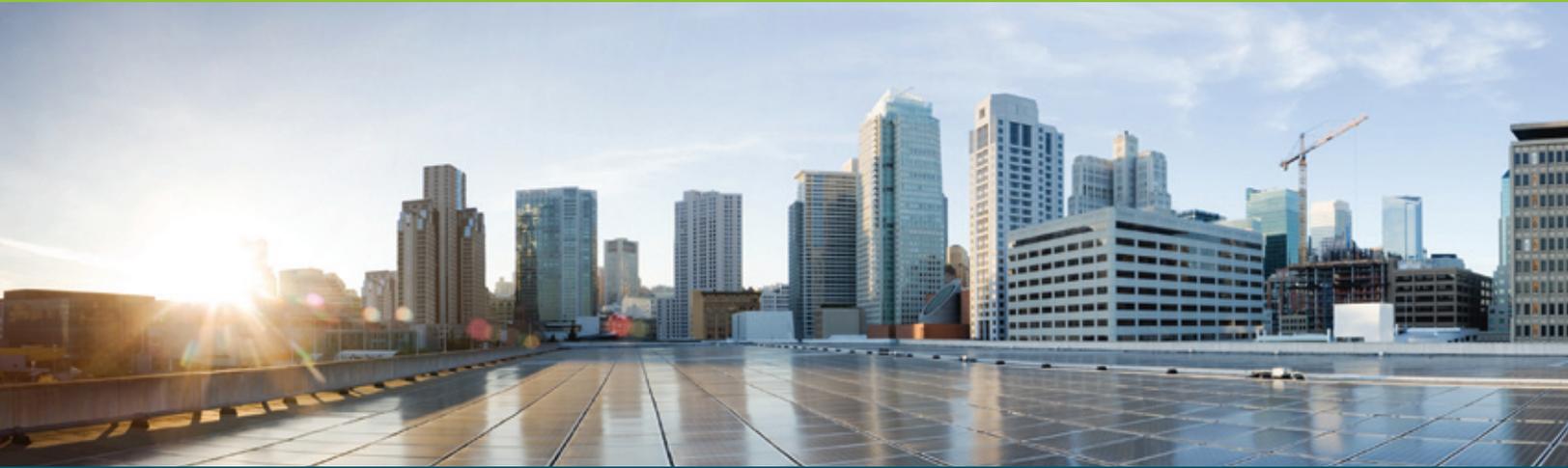
When it comes to enforcing security policies in the enterprise, 62 percent of IT decision-makers surveyed said employee training is their top approach, followed by:

- URL filtering (57 percent)
- Monitoring only (41 percent)
- Data loss prevention technology (39 percent)

*More than one answer allowed.

In addition, the majority of Cisco survey respondents from China and India (71 percent) said they recognize that overly strict security policies can have a negative impact on hiring and retention of employees who are under the age of 30 (Generation Y). But roughly four in 10 IT security decision-makers in Germany (39 percent) and Japan (42 percent) perceive that restrictive policies will have no impact at all on attracting and keeping employees from the Generation Y demographic pool.

Five Ways Enterprises Can Strengthen Their Security by 2011



While most organizations are grappling with the same forces of change—the proliferation of mobile and connected devices, virtualization and cloud computing, and trends such as social networking that are transforming the way employees collaborate and communicate—they do not necessarily face the same security challenges.

An organization's network infrastructure, and the security that supports it, is a complex ecosystem that is always changing. What and whom the business needs to protect varies as well. Each new event—whether a merger or acquisition, hiring or downsizing, or a new product launch—has an impact on what the enterprise needs to protect.

However, in addition to the advice presented throughout this report, there are several steps that businesses, with guidance from their IT teams, and involvement and support from their employees, can take to strengthen their enterprise security within the next six months. These measures will help the organization respond to the tectonic forces of change now in motion, and to build a foundation that will allow it to adapt more readily to future changes that affect enterprise security.

1

Close Gaps in Situational Awareness

“Moment by moment” awareness of the state of the network is needed because the enterprise is in a constant state of change—you acquire a new company, hire new employees, change applications, and add new devices. Most enterprises are simply not aware of the totality of their network: There are outliers—disconnected elements—that present real risk. There are many moving parts and areas of low visibility to monitor and manage, such as mobile workers, mobile devices, web-based collaborative applications, and the cloud.

By taking stock of these elements, IT teams gain better visibility into the overall network security posture. They also can identify and correct weaknesses more easily, and remove or block those things that should not be connecting to the network. Unfortunately, many IT departments, especially those whose budgets were cut when the economy stumbled, are focused primarily on blocking immediate threats or patching major vulnerabilities. (Important steps, to be sure, but not enough.) There often isn't enough time or money for thorough reconnaissance of network practices. And executives may not encourage IT to spend time implementing practices that don't appear to have an immediate return on investment.

Most enterprises are simply not aware of the totality of their network.

Yet enterprises are likely to save time and money when they do step back and assess whether simple steps are being pursued to reduce vulnerabilities. These actions require front-end investment in “people resources” (the costs come from employee time, not from hardware or software purchases). But it's an investment that pays off down the road when vulnerabilities are disclosed, and the IT department can

spend less time checking to see if certain networked devices are not patched or configured in such a way to make them affected by the recently disclosed vulnerabilities.

For instance, networking systems often have little-used, unneeded, or insecure features or services enabled by default, such as Telnet, TFTP, or certain DNS services. As Cisco has noted in previous security reports, cybercriminals are endlessly creative when it comes to finding new ways to launch attacks, and will even use “old school” methods (such as exploiting past vulnerabilities) that they believe will escape detection. Proactive IT departments will disable unused services, such as operating system add-ons, to avoid future malware infections.

And to avoid a scenario in which certain network devices drop off the radar of network control, enterprises should adopt a change-control approach to managing devices. In other words, several stakeholder groups—such as desktop, network operations, and IT security—need to all be informed when a device is made active on the network, as well as when it has been removed from use.

2

Focus First on Solving “Old” Issues—and Doing It Well

Many of the security issues considered to be “new” problems are actually old issues that can be managed and secured using existing, effective practices. One word of caution, however: Organizations should start by working to solve a limited number of things—and doing them well—instead of trying to solve too many problems at once, only to arrive at mediocre results or unfinished projects.

Software updating and patching is a good place for many organizations to begin making improvements: Enterprises have steadily lost control over the software that's installed on technology assets. The task of managing what software

employees could use, and what programs were forbidden, was much easier when networks were closed, IT staff could touch each and every desktop and laptop computer, and employees only worked when they were using a corporate-approved device.

Software updating and patching is a good place for many organizations to begin making improvements.

With today's unwieldy networks comprised of a mix of officially sanctioned technology equipment, and whatever mobile devices workers have decided suit their needs, enterprises can't guarantee that everyone is using approved versions of corporate software. Employees, like computer users everywhere, are likely to ignore constant reminders to upgrade to the latest version of the Microsoft Internet Explorer or Mozilla Firefox browsers. Nor can enterprises assume that all software has been properly patched.

In addition, executives may not have come to the realization that software development cycles have shortened for many vendors. While new versions of software formerly were released on a semi-yearly or yearly basis, some vendors, including Adobe, Apple, and Microsoft, are delivering patches and updates more frequently. For instance, in the first three months of 2009, Microsoft announced 58 vulnerabilities; in the first three months of 2010, the company announced 77 vulnerabilities. In the same time period in 2009, Adobe announced nine vulnerabilities; in the first three months of 2010, 26 vulnerabilities. (In the first three months of 2009, Cisco announced 45 vulnerabilities; and in the first three months of 2010, the company announced 44 vulnerabilities.) Adobe executives recently indicated that they would consider reducing the time frame between security updates for its Adobe Reader product from 90 days to 30 days, in part because of the increase in vulnerabilities.

It is essential for enterprises to monitor the vulnerability disclosures of their key vendors and be ready to act accordingly to reduce potential exposure to new vulnerabilities. This process should include informing employees. Without implementing these frequent updates, workers are increasing the likelihood of falling victim to exploits that are delivered via software vulnerabilities. Criminals are as innovative as software developers, and are continually on the alert for new ways to hack into a network or launch an executable malware file via an unpatched piece of software.

The solution to the outdated software problem is to develop a system for centralized management of approved software, and for delivering updates. For instance, automated patching and software updates eliminate the reliance on workers to carry out these crucial tasks. In addition, enterprises can offer software configuration support on a centralized basis for all IT-supported platforms.

However, recognizing the difficulty of thorough management of updating and patching, it may make more sense for enterprises to implement other measures that serve a similar purpose. "Businesses should expand their view of vulnerability management to include easily applied leading practices and mitigations that can relieve some of the strain on updating and patching," says Russell Smoak, senior director of Cisco Security Research and Operations. "For example, blacklisting, whitelisting, and ingress and egress filtering are all easier to apply, update, and control than deploying patches and updates across an enterprise." What's more, they can provide the luxury of additional time to deploy upgrades and patches, without leaving critical resources unprotected.

3

Educate Your Workforce on Security—and Include Them in the Process

Allow users to be part of the security solution by encouraging bidirectional communication about security issues. When educating users, explain the security issues the enterprise needs to address, and ask them how they can help the organization to solve these problems. The most effective training uses real-world examples of criminals and attacks to show employees that threats are genuine and can cause significant damage.

Be sure to target C-level and other VIPs for extensive education, as they are prime targets for phishing and social engineering schemes designed to connect hackers with sensitive business information (see the *Downside of Being a VIP (or Just Working for One)*, page 22). Enterprises also

should enlist their millennial workforce in their efforts to improve security. Gen Y employees are often more comfortable and familiar with popular technology, such as social networking, and can help workers from other generational groups learn how to navigate such technology and use it appropriately—once millennial employees themselves have been fully educated on the enterprise's security policy, of course.

Target C-level executives and other VIPs for extensive education, as they are prime targets for phishing and social engineering schemes.

While most users (of any generation) have become savvier about not clicking on suspect links from Facebook friends or within an instant chat message, there is evidence that Generation Y is a bit sloppy about revealing sensitive business and personal information across these networks. According to a recent study by Accenture, "Millennials have a much looser notion of online privacy than do older workers," with 30 percent of millennials saying that they write openly about themselves online.

This casual approach to sharing personal information has become more of a threat than suspect links in emails from supposed "friends." Since criminals are honing their skills in gathering available data on a business or its top executives to launch an attack, indiscreet chat about upcoming product launches or personnel changes can cause more damage than ever. The website WikiLeaks.org, which publishes leaked information from government organizations and corporations, has collected more than 1 million documents—apparently, sensitive data is not all that difficult to find.

"Workers need to have a heightened awareness of the pain they can cause a business when they over-share information via social networks," advises Seth Hanford, Intelligence Operations Team Lead at Cisco. "They may be unaware that they could put customers, their own jobs, and others at risk, along with the enterprise's ability to turn a profit. Executives need to clearly state the ramifications of workers' actions."

In addition to properly advising users about the impact of sharing business information, enterprises need to shift their thinking about security toward a "culture of yes." Instead of banning all social networking in a bid to improve security, for example, the enterprise should take steps to protect data as it moves through these networks.

Hanford concludes, "If users don't know what is expected of them, one should have no expectation that they will take the right steps to protect the data that the enterprise needs to safeguard."

4

Understand That One Security Border Is No Longer Enough

IT professionals used to focus on finding better, more efficient ways to fortify the security border that protected the network. All the applications an employee needed for work were located within the network, which they accessed from a corporate-issued device and from within the corporate office. The security threats they encountered came from outside the network, via email or web traffic. But now, business is becoming "borderless" and so, too, is the network, which means there are multiple borders to protect instead of just one, and they are constantly changing.

This report outlines the tectonic forces of change bringing forth the borderless enterprise. Employees are accessing the network and sharing data through an array of mobile devices and web-based applications. Services, functions, and business operations are being externalized. The "fortress" approach to security of the past clearly is no longer adequate. With workers collaborating and sharing vital information far beyond the walls of the workplace, every hour of every day, security that's limited to the network edge is bound to fail.

More than that, today's hackers are skilled at breaking through traditional security perimeters and are finding it all too easy to penetrate the "soft spots" in the enterprise where sensitive data resides and is not protected by any security border (see *Insight from the Security Researchers: Hackers Are Choosing Their Own Adventure*, page 20). Never before has it been more important for enterprises to adopt a layered approach to security, and to make certain that wherever critical data flows or resides, it is protected by intelligent technology solutions, rich policies, robust enforcement practices, and a workforce who has been educated about security risks and who understand their role in helping to mitigate them.

Business is becoming "borderless," and so, too, is the network, which means there are multiple borders to protect... and they are constantly changing.

5

View Security as a Differentiator for Your Business

Strengthening enterprise security should never be a back-burner agenda item for businesses. It is an asset—and in many ways, it can be a competitive tool. Leading organizations are aligning their security investments with their business objectives and finding that it allows them to adapt more quickly and confidently to changing business conditions, take advantage of new technologies and markets, and enhance the customer experience.

How an enterprise approaches security and responds to trends such as social networking and mobility can have a direct impact on its ability to hire and retain talent.

Many businesses are also beginning to fully recognize the importance of protecting their data, regardless of where it resides or moves. And they are realizing that by strengthening their enterprise security, they can ensure compliance with industry and government regulations and reduce the risk of litigation from data loss or security breaches. Ultimately, a proactive approach to security can help to preserve the company's reputation and protect its financial assets.

How an enterprise approaches security and responds to trends such as social networking and mobility can also have a direct impact on its ability to hire and retain talent, particularly from the Gen Y demographic pool. Robust security practices allow businesses to provide employees with the widest appropriate levels of access to the tools and applications they need to work remotely—as well as effective defenses against inappropriate use or unauthorized access.

Inadequate, outdated security, meanwhile, poses a significant risk to the enterprise and its assets, from intellectual property to devices to employees—and customers and business partners as well. And if those who do, or would like to, conduct business with your organization have not yet inquired about your company's security policies, processes, and practices, be assured that they will.

Network and IT systems make up some of an organization's most critical infrastructure. Together, they are the "endoskeleton" supporting the business and protecting its data. And like a living thing, if that vital framework is neglected, it will surely fail—especially when under pressure. The tectonic forces are creating unprecedented stress on the enterprise: Businesses must take action now to test the robustness of their infrastructure and implement effective security practices so they can endure—and thrive—in the new landscape formed by these changes.

It is important for enterprises to recognize, however, that there is no "silver bullet" technology solution that can meet all their security needs. A layered approach that includes depth and breadth of defense is the only way to meet the challenges and protect the opportunities presented to the enterprise by these forces of change and the emerging borderless network.



Security Trends: Midyear Notes

In each Cisco Security Report, Cisco security experts combine their knowledge and insight to make educated predictions about security threats and trends that are likely to be significant in the next six to 12 months, taking into account emerging trends and recent activity by the cybercriminal community—both in terms of user behavior and attack methods and exploits. Following are a few of the trends discussed in the *Cisco 2009 Annual Security Report*²², and some recent developments since the report was published.

Spam Volume is Expected to Rise Up to 30 Percent Worldwide Over 2009 Levels

According to new research compiled by Cisco Security Intelligence Operations (SIO), spam volume worldwide is on track to rise by up to 30 percent over 2009 levels. However, it should be noted that spam volume was lower than might have been expected in the first six months of 2009 because worldwide spam volume plummeted following the takedown of Internet hosting provider, McColo, which hosted the Reactor Mailer command-and-control infrastructure that controlled the Srizbi/Reactor Mailer botnet.

The latest figures from Cisco SIO show that the United States is once again the spam leader among countries worldwide, pushing Brazil down to third place after the country occupied the top position for only a few months. Overall spam volume actually declined for both countries in the period from November 2009 through June 2010—but the percentage of global spam from Brazil decreased much more than that from the United States (Brazil, -4.30 percent; the United States, -0.56 percent). Cisco security experts suspect the decrease in Brazil's spam volume could be related to more Brazilian ISPs limiting Port 25 access, an important spam-blocking technique.

India, meanwhile, moves up to second place from third. Since the end of 2009, there has been only a modest increase in the percentage of global spam originating from that country (+1.10 percent). Russia leaps from ninth place to fourth among spam-originating countries, even though its percentage of global spam volume actually declined slightly during the first six months of 2010 (-0.26 percent).

Spam Trends by Originating Country
November 2009 – June 2010

Country	Percentage of Global Spam	Spam Trend
United States	8.98%	-0.56%
India	8.61%	1.10%
Brazil	6.71%	-4.30%
Russia	6.43%	-0.26%
South Korea	3.83%	-0.86%
Vietnam	3.74%	-1.65%
Ukraine	3.60%	0.53%
Germany	3.34%	1.99%
China	3.22%	-1.19%
Italy	2.80%	1.30%
United Kingdom	2.74%	2.39%
Colombia	2.58%	-1.30%

Source: Cisco Security Intelligence Operations

²² Cisco 2009 Annual Security Report, www.cisco.com/en/US/prod/collateral/vpndevc/cisco_2009_asr.pdf.

Vietnam, which had a peak in spam volume during the October to November 2009 time frame, retains its position at sixth place, while its spam levels continue to trend down. The country's global spam levels declined by 1.65 percent in the period from November 2009 to June 2010.

After experiencing similar spikes in their spam volume during the same period last fall, South Korea and Turkey—both in the top five at the end of 2009—saw their percentage of global spam volume drop in the first half of 2010. South Korea had only a slight decrease (-0.86 percent) and has moved to fifth position from fourth place. But Turkey's spam volume has declined so much that it is now ranked 25th among spam-originating countries worldwide, according to research from Cisco SIO.

Falling off the list since December 2009, in addition to Turkey, are Argentina and Poland. And moving into the top 10 since the end of last year are Colombia, Germany, Italy, Ukraine, and the United Kingdom. Of those five countries, the United Kingdom has seen the greatest increase (+2.39 percent) over the past six months in the percentage of global spam volume that it originates; Germany had the second highest increase (+1.99 percent) among the newcomers to the list.

Meanwhile, in the first half of 2010, China fell two spots on the list to ninth place. While there was a significant reduction (-24.3 percent) in the percentage of global spam originating from China during 2009, the trend decrease has been slight (-1.19 percent) since November 2009.

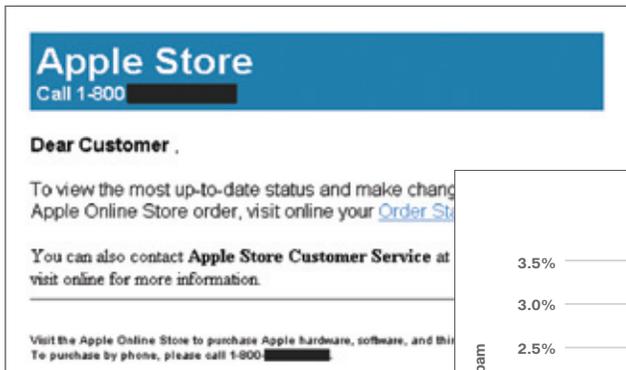
More Attacks on Legitimate Websites

Cybercriminals are still targeting legitimate websites—but some are now employing them in multivector attacks with a focus on spam. In late March, attackers sent a wave of spam messages targeting customers of the highly popular Apple Store. The attackers, which strategically timed their campaign just before the launch of Apple's iPad, coordinated their attacks with thousands of legitimate websites and spam imitating an Apple Store notice with links to the compromised websites. The attack also redirected compromised traffic to a Canadian pharmacy website, which served up a fake anti-virus Trojan.

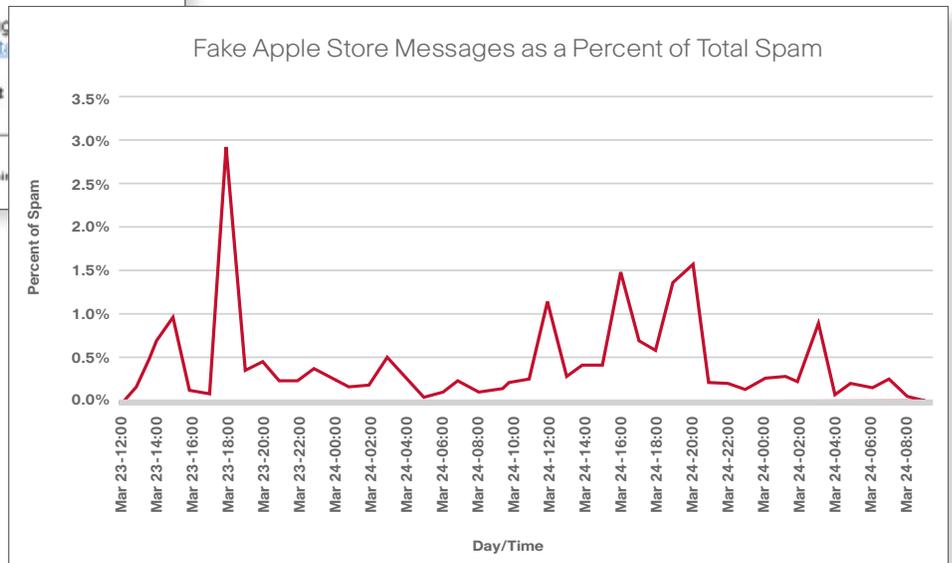
Social Networks: A Cybercrime Hotspot for 2010

While social networking worms appear to have decreased since the publication of the *Cisco 2009 Annual Security Report*, attacks using social media have increased—and new threats are emerging. One particularly disconcerting trend is that social networks are now attracting a more dangerous criminal element: terrorists. (See *Taking Action to Reduce Innovation Gaps*, page 16).

The U.S. government is concerned enough about social networking's role as a tool for terrorists that the U.S. Army Research Laboratory recently provided a nearly US\$17 million, five-year grant to Rensselaer Polytechnic Institute to examine how social networks and other technology, including smartphones, can be used to organize, coordinate, and incite potential attacks against the United States.²³



Leveraging the highly anticipated release of Apple's iPad tablet PC, multiple waves of email spam were sent worldwide in an effort to dupe recipients who may have pre-ordered the iPad and wanted to check their latest availability status.



23 "When Social Sites Are Weapons," by Larry Rulison, TimesUnion.com, May 5, 2010, www.timesunion.com/AspStories/story.asp?storyID=928058&category=RENSSELAER.



Cisco Security Intelligence Operations

Cisco Security Intelligence Operations (SIO) is an advanced security infrastructure that enables the highest level of security and threat detection and prevention for Cisco customers. With sophisticated security intelligence, more than 750,000 sensors deployed worldwide, automated update systems, and a team of global research engineers, threat experts, statisticians, and analysts, as well as 76 patents and 250 certifications, Cisco SIO helps organizations gain visibility into the latest threat landscape and plays a critical role in helping Cisco to secure borderless networks for customers worldwide.

It has become an increasing challenge to manage and secure today's distributed and agile networks. Cloud computing and the sharing of data are threatening security norms. Online criminals are continuing to exploit users' trust in consumer applications and devices, increasing the risk to organizations and employees. Traditional security, which relies on layering of products and the use of multiple filters, is not enough to defend against the latest generation of malware, which spreads quickly, has global targets, and uses multiple vectors to propagate.

Cisco SIO, a cloud-based service, uses three components that enhance the filters already available in Cisco devices:

- **Cisco SensorBase®.** The world's largest threat-monitoring network, Cisco SensorBase captures global threat telemetry data from an exhaustive footprint of Cisco devices and services—this includes more than 1 terabyte of data per day and 30 percent of the world's email traffic.
- **Cisco Threat Operations Center:** A global team of security analysts and automated systems that extract actionable intelligence. Additionally, Cisco "White Hat" engineers provide services such as penetration testing, botnet infiltration, and malware reverse engineering.
- **Dynamic updates:** Real-time updates are automatically delivered to security devices, along with effective practice recommendations and other content dedicated to helping customers track threats, analyze intelligence, and, ultimately, improve their overall enterprise security posture.

Cisco is committed to providing complete security solutions that are integrated, timely, comprehensive, and effective—enabling holistic security for organizations worldwide. With Cisco, organizations can save time researching threats and vulnerabilities, and focus more on taking a proactive approach to security.

For more information on Cisco SIO, visit www.cisco.com/go/sio.

Cisco Security IntelliShield Alert Manager Service provides a comprehensive, cost-effective solution for delivering the vendor-neutral security intelligence organizations need to identify, prevent, and mitigate IT attacks. This customizable, web-based threat and vulnerability alert service allows security staff to access timely, accurate, and credible information about threats and vulnerabilities that may affect their environments. IntelliShield Alert Manager allows organizations to spend less effort researching threats and vulnerabilities, and focus more on a proactive approach to security.

Cisco offers a **free 90-day trial** of the Cisco Security IntelliShield Alert Manager Service. By registering for this trial, you will have full access to the service, including tools and threat and vulnerability alerts.

To learn more about Cisco Security IntelliShield Alert Manager Services, visit: <https://intellishield.cisco.com/security/alertmanager/trial.do?dispatch=4>

For More Information

Cisco Security Intelligence Operations

www.cisco.com/security

Cisco Security Blog

blogs.cisco.com/security

SenderBase

www.senderbase.org

Cisco Security Services

www.cisco.com/go/ros

www.cisco.com/go/intellishield

Cisco Security Products

www.cisco.com/go/security

www.cisco.com/go/asa

www.cisco.com/go/ips

www.ironport.com

www.scansafe.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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)