Cisco 2011 Annual Security Report

HIGHLIGHTING GLOBAL SECURITY THREATS AND TRENDS

cisco

The *Cisco® Annual Security Report* provides an overview of the combined security intelligence of the entire Cisco organization. The report encompasses threat information and trends collected between January and November 2011. It also provides a snapshot of the state of security for that period, with special attention paid to key security trends expected for 2012.

PART 1

PART 2

PART 1

Welcome to the Connected World

Imagine the 1960s office of the fictional advertising agency portrayed on the American television show "Mad Men": When it came to technology, workers could avail themselves of typewriters and telephones (both operated largely by the secretarial pool)—which were basically all they had in the way of productivity-enhancing equipment. Employees attended perhaps one or two meetings a day; work began when people arrived at the office, and stopped when they went home.

Today's workers get more done over breakfast or during the morning commute than their 1960s predecessors accomplished in an entire day. Thanks to the array of technology innovations flooding into the workplace—everything from tablets to social networking to video-conferencing systems such as telepresence—employees can work almost anywhere and anytime they need to, provided the right technology is there to support connectivity and, even more importantly, provide security. In fact, the modern workplace may differ from its 1960s counterpart most dramatically in terms of the lack of actual people: Showing up at the office is less and less necessary.

Along with the onslaught of technology innovations, there's also been a shift in attitude. Today's workers have become so accustomed to the productivity benefits and ease of use of their devices, social networks, and web applications that they see no reason why they can't use all these tools for work as well as for play. The boundaries between work and home are nearly nonexistent: These workers chat with their supervisors on Facebook, check work email on Apple iPads after watching a movie with the kids, and turn their own smartphones into mini-workstations.

Unsurprisingly, many enterprises are questioning the impact of technology innovation and flexible work habits on corporate information security—and sometimes, take the drastic step of banning devices or restricting access to web services that workers say they need (and do need, in most cases). But organizations that don't allow workers this flexibility—for instance, allowing them to use only a given company-owned smartphone—will soon find they can't attract talent or remain innovative.

Research conducted for the *Cisco Connected World Technology Report* study (www.cisco.com/en/US/netsol/ns1120/index.html) documents changing attitudes toward work, technology, and security among college students and young professionals around the globe, who are driving the next waves of change in the enterprise. (Workers of all ages have been responsible for increasing adoption of consumer devices in the workplace and anytime/anywhere information access, but younger workers and new graduates are drastically speeding up the pace of change.) This year's edition of the *Cisco Annual Security Report* highlights many key findings from this research, exploring the impact on enterprises and suggesting strategies for enabling innovation.

For instance, most college students (81 percent) surveyed globally believe they should be able to choose the devices they need to do their jobs—either by having their employers pay for them or bringing their own personal devices to work. In addition, almost three-quarters of students surveyed believe they should be able to use such devices for both business and personal use. Multiple devices are becoming commonplace: 77 percent of surveyed employees worldwide have multiple devices in use, such as a laptop and a smartphone or multiple phones and computers. (See "Your Future Workers: Loaded with Devices, and Not Overly Concerned About Security," page 5.)

A Balanced, Flexible Approach to Security

Trends such as the influx of consumer devices in the workplace will require more flexible and creative solutions from IT staff for maintaining security while enabling access to collaborative technologies. Given the desire of workers to bring the devices they use at home into the workplace, enterprises need to adopt a "bring your own device" (BYOD) vision—that is, securing the network and data regardless of how workers access information. (See "Remote Access and BYOD: Enterprises Working to Find Common Ground with Employees," page 10.)

"Today's IT departments need to enable the chaos that comes from a BYOD environment," says Nasrin Rezai, Cisco's senior director of security architecture and chief security officer for the Collaboration Business Group. "This doesn't mean accepting high levels of risk, but being willing to manage some risks in exchange for attracting talent and delivering innovation. It's about moving to a world in which not every technology asset can be managed by IT."

A willingness to balance risks and benefits is a hallmark of IT's new posture toward security. Instead of outright bans on devices or access to social media, enterprises must exchange flexibility for controls that workers agree to. For instance, IT staff may say, "You can use your personal smartphone to read and respond to company email, but we need to manage that asset. And if you lose that phone, we'll need to erase data remotely, including your personal apps and pictures of your family."

Workers must be part of this compromise: They need to see the value of cooperating with IT so they can use the tools they have come to rely on—and help lay the groundwork for a process that will enable faster adoption of new technologies in the workplace as they emerge.

Another fundamental adjustment by enterprises and their security teams is the acceptance of the public nature of business. According to the *Connected World* study, young professionals and students see far fewer boundaries between work life and personal life: 33 percent of college students say they don't mind sharing personal information online.

"The older generation assumes everything is private, except what they choose to make public," explains David Evans, chief futurist for Cisco. "To the younger generation, everything is public, except what they choose to make private. This default position—that everything is public—goes against how enterprises have worked in the past. They've competed and innovated based on protecting their information from being exposed. However, they need to realize that the benefits they receive from sharing information are greater than the risks of keeping information within their walls."

The good news for IT is that their role as enablers of collaboration and sharing should lead to greater responsibility—and hopefully, more budget—for the enterprise's growth and development. "Success is when IT can enable these dramatic changes in the workplace, not inhibit them," says John N. Stewart, vice president and chief security officer for Cisco. "We should not focus on specific issues, like whether to allow people to use their iPads at work, because it's a foregone conclusion. Rather, focus on solutions to the bigger business challenge: enabling technology for competitive advantage."

Your Future Workers:
Loaded with Devices, and Not Overly Concerned About Security

Ten years ago, employees were assigned laptops and told not to lose them. They were given logins to the company network, and told not to tell anyone their password. End of security training.

Today, your "millennial" employees—the people you want to hire because of the fresh ideas and energy they can bring to your business—show up to their first day on the job toting their own phones, tablets, and laptops, and expect to integrate them into their work life. They also expect others—namely, IT staff and chief information officers—to figure out how they can use their treasured devices, anywhere and anytime they want to, without putting the enterprise at risk. Security, they believe, is not really their responsibility: They want to work hard, from home or the office, using social networks and cloud applications to get the job done, while someone else builds seamless security into their interactions.

Research from the *Connected World* study offers a snapshot of how younger workers and college students about to enter the workforce view security, access to information, and mobile devices. Here's a snapshot of who you'll be hiring, based on findings from the study:

81% OF COLLEGE STUDENTS BELIEVE THEY SHOULD BE ABLE TO CHOOSE **THE DEVICES THEY NEED** TO DO THEIR JOBS

Source: *Cisco Connected World Technology Report*

Social Media: Now, It's a Productivity Tool

Facebook and Twitter long ago moved beyond mere novelty sites for teens and geeks, and became vital channels for communicating with groups and promoting brands. Young professionals and college students know this, and weave social media into every aspect of their lives. (And while Facebook and Twitter are the dominant players in much of the world, many other regional social networks are becoming just as essential to online interaction—for instance, Qzone in China, VKontakte in Russia and former Soviet-bloc countries, Orkut in Brazil, and Mixi in Japan.)

However, enterprises may not understand the extent to which social media has made inroads into the public and private lives of their employees, especially younger workers—and therefore, do not feel the need to yield to growing demand in their workforce for unfettered access to social networks like Facebook or content-sharing sites such as YouTube. Unfortunately, this inertia may cost them the talent they need to grow and succeed. If access to social networks isn't granted, young professionals who expect to have it are likely to seek work at companies that do provide such access. These attitudes are even more prevalent among college students, who have been using social media from a young age.

According to research for the *Connected World* study, college students and young workers center their social and business interactions around Facebook. Eighty-nine percent of college students surveyed check their Facebook page at least once a day; seventy-three percent of young professionals do so as well. For young workers, their social media connections often extend into the workplace: Seven out of 10 employees said they have friended managers or co-workers on the social media site.

Given their level of activity on Facebook—and the lack of distinction between personal and business use of the social media site—it stands to reason that young workers want to carry their Facebook use into the office. Among college students surveyed, almost half (47 percent) said they believe companies should maintain flexible social media policies, presumably to allow them to stay connected in their work and personal lives at any time.

If students encounter a workplace that discourages social media usage, they may avoid these companies altogether—or if they're stuck working in these environments, they may try to subvert the rules blocking access to their favorite sites. More than half of college students surveyed globally (56 percent) said if they encountered a company that banned access to social media, they would either not accept a job there, or would join and then find a way to access social media despite corporate policies. Two out of three college students (64 percent) said they plan to ask about social media usage policies during job interviews, and one in four (24 percent) said such policies would be a key factor in their decision to accept a position.

The Upside of Social Media Access

Since social media is already so entrenched in the daily lives of young professionals and future workers, enterprises can no longer view it as a passing nuisance or a negative, disruptive force. In fact, companies that block or narrow access to social media likely will find themselves at a competitive disadvantage.

When enterprises accept social media use by the workforce, they are providing their employees with the tools—and the culture—they need to be more productive, innovative, and competitive. For example, hiring managers can use social networks to recruit new talent. Marketing teams can monitor social media channels to track the success of advertising campaigns or consumer sentiment about brands. And customer service teams can respond to consumers who use social media to ask questions and provide feedback to companies.

Fears around security and data loss are a leading reason why many businesses don't embrace social media, but these concerns are likely out of proportion with the true level of risk (see "Myth vs. Reality: Social Media Is Dangerous to the Enterprise" on facing page); in any case, risks can be mitigated through the application of technology and user controls. For instance, web traffic controls can halt malware such as Koobface[1] that finds

[1] "The Evolution of Koobface: Adapting to the Changing Security Landscape," Cisco 2010 Annual Security Report, www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf.

its way through Facebook and Twitter. These controls don't inhibit workers from browsing social media and using it to connect with colleagues, customers, and business partners. They are stopped from social media activity only when they are in danger of downloading an infected file or clicking on a suspicious link. The protection is invisible to users, and is built into the network, not computers or devices. Workers get the social media access they demand, and businesses get the information safety they require. (See more on social media protections in "The Future for Acceptable Use Policies," page 19.)

Social media sites themselves have responded to requests to offer greater levels of control over what users can see within a network. For example, a business can allow workers to access YouTube to view videos related to its industry or product, but block access to adult content or gambling sites. And technology solutions can filter social media traffic for incoming malware or outgoing data (for instance, company files that should not be emailed via social media or other web-based services).

To protect a business's users against unauthorized access to their accounts, Facebook has steadily introduced privacy features. While these are individual user controls as opposed to network controls, businesses can engage in discussion with workers and offer training about the most useful privacy features for maintaining information security.

Before limiting access to social media, enterprises should consider the business value of social media versus the risk of allowing it. Considering the findings of the *Connected World* study and the passion young workers have for social media and its collaborative powers, businesses are likely to discover the benefits outweigh the risks—provided they find the right balance between acceptance and security.

Myth vs. **Reality**: Social Media Is Dangerous to the Enterprise

Myth:
Allowing employees to use social media opens the door wide to malware in the company network, and will cause productivity to plummet. In addition, employees will divulge company secrets and inside gossip on Facebook and Twitter, damaging the enterprise's competitive position.

Reality:
There's no doubt that criminals have used social media networks to lure victims into downloading malware and handing over login passwords. But the fear of threats delivered via social media may be overblown. Email messages remain the most popular way to get malware into networks.

Certainly, enterprises should be concerned about loss of intellectual property, but social media doesn't deserve full blame for such losses. Employees who haven't been trained to protect their employer's information can unleash secrets by indiscreet chats in public places or via email as fast as they can tweet, and they can download company documents onto thumb drives as easily as trading information over Facebook email. The answer to IP leakage is not an outright ban on social media. It's imbuing trust in the workforce so workers don't feel compelled to disclose sensitive information.

"The loss of productivity due to social networking has been the subject of many media scare stories," says Jeff Shipley, manager of Cisco Security Research and Operations. "However, the truth is that employees can do more work, and do so better and faster, when they use tools that let them rapidly collaborate on projects and talk to customers. Today, social media networks are those tools. The productivity gains make up for the occasional downtime inherent in social networking."

> "The truth is that employees can do more work, and do so better and faster, when they use tools that let them rapidly collaborate on projects and talk to customers."
>
> —Jeff Shipley, manager of Cisco Security Research and Operations

Remote Access and BYOD:
Enterprises Working to Find Common Ground with Employees

While the question of whether to allow employees to access social media during work hours and with company assets is top of mind for many organizations, a more pressing concern is finding the right balance between allowing their employees to have access to the tools and information they need to do their jobs well–anytime, anywhere–while also keeping sensitive corporate data, such as intellectual property and employees' personal information, secure.

Enterprises across industries are starting to understand they must adapt soon to "consumerization of IT" (employees' introduction and adoption of consumer devices in the enterprise) and the remote working trends already under way in their organizations. It is becoming increasingly clear that if they don't change, they cannot stay competitive, innovate, maintain a productive workforce, and attract and keep top talent. At the same time, they are realizing that maintaining previously defined security borders is no longer possible. "IT organizations, particularly those in large companies, have not been able to keep pace with the Internet-speed growth of new devices and the immediate adoption of those devices by employees–especially younger workers," says Gavin Reid, Computer Security Incident Response Team (CSIRT) manager for Cisco.

There clearly is an expectation among tomorrow's young professionals–as well as many of today's–that they will be able to access whatever they need from wherever they are in order to do their jobs. And if they aren't provided with that access, the consequences for the enterprise are potentially significant. As an example, the *Connected World* study revealed that three in 10 young professionals globally admit that the absence of remote access would influence their job decisions, such as leaving an existing job sooner than later or declining job offers outright. They also indicate they would be more likely to slack off while on the job and experience lower morale.

As for today's college students, most can't even imagine a future work experience that did not include the ability to access work remotely. According to the *Cisco Connected World Technology* survey, nearly two in three college students expect that, when they are in the workforce, they will be able to access their corporate network using their home computer. Meanwhile, about half of college students expect to do the same using their personal mobile devices. And more than likely, if the enterprise does not allow them to do these things, these future workers will find a way to overcome obstacles to access.

The report also reveals that most college students (71 percent) share the view that company-issued devices should be available for both work and play because "work time often blends with personal time … It's the way it is today and the way it will be in the future." That latter statement is very true, which is why more enterprises are moving to implement a BYOD practice. Other factors, including workforce mobility, the proliferation of new

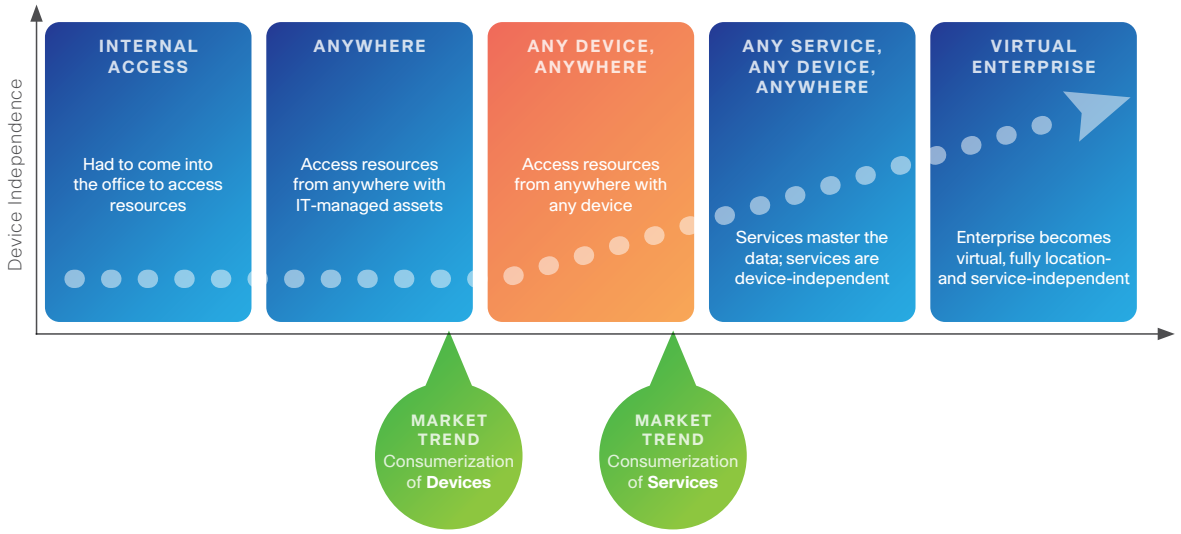


Figure 1. The Stages of Workforce Access Along the Any Device Journey

devices, and acquisition integration and management of offshore and offsite outsource relationships, are also key drivers.

Cisco is one organization already making the transition to BYOD—and is learning quickly that this transformation requires both long-term commitment and cross-functional engagement in the organization. Depicted in Figure 1 on the previous page are the five stages of workforce access along what Cisco calls its "Any Device" journey toward becoming a "virtual enterprise." By the time Cisco reaches the last stage of its planned journey, which will take several years, the organization will be increasingly location- and service-independent—and enterprise data still will be secure.[2]

The specific demands of an organization's industry segment (regulatory demands) and corporate culture (risk tolerance versus innovation) drive BYOD decisions. "I think for many organizations today, the BYOD issue is less a matter of 'No, we can't do it' and more a question of '*How* do we do it? What positive, responsive actions should we take to manage the mobile device situation in our organization?'" says Nasrin Rezai, Cisco's senior director of security architecture and chief security officer for the Collaboration Business Group.

One common theme among organizations moving toward the practice of BYOD is that there is buy-in from top executives who are helping not only to bring the matter to the forefront in the company, but also

Technology Making a Safer Journey to BYOD for Cisco

As part of the decision to allow employees to use any device for work, including unmanaged personal devices, Cisco IT, along with CSIRT, sought a tool that would block malicious websites before they loaded onto browsers. In short, they wanted protection against zero-day threats—specifically those without a known signature. However, the solution also needed to preserve the user experience—not only to ensure productivity, but also to prevent employees from changing their browser settings.

Cisco IT and CSIRT achieved their goal by deploying the Cisco IronPort® S670 Web Security Appliance (WSA), a web proxy that inspects and then either forwards or drops web traffic based on reputation filters or the outcome of inline file scanning. (Cisco does not use the WSA's web-filtering capabilities to block entire website categories because its policy is to trust employees to use their time productively.)

When a Cisco employee clicks a link or enters a URL, the request is sent by way of Web Cache Communication Protocol (WCCP) to a load-balanced pool of Cisco IronPort S670 WSAs. The WSA

determines whether to allow or reject the entire website, or individual objects on the website, based on a reputation score from the Cisco IronPort SenderBase® Security Network (www.senderbase.org) cloud-based email and web traffic monitoring service. SenderBase assigns each website a reputation score ranging from –10 to 10. Websites with scores from –6 to –10 are blocked automatically, without scanning. Websites with scores from 6 to 10 are allowed, also without scanning.

Cisco deployed the Cisco IronPort S670 WSA throughout its organization in three phases, which began with a six-month proof-of-concept program in one building of the Cisco campus in Research Triangle Park (RTP), North Carolina, followed by a two-year pilot program (2009–2011) in which the solution was extended to all 3000 employees at the RTP campus. In 2011, the WSA was rolled out to other large campus sites worldwide and tens of thousands of employees. As of November 2011, Cisco's global WSA deployment is 100 percent complete.

"Cisco is now experiencing its highest-ever level of protection from web-based threats," says Jeff Bollinger, senior information security investigator for Cisco. "We average 40,000 blocked transactions per hour. And in just one day, the WSAs blocked 7.3 million transactions, including 23,200 Trojan downloader attempts, over 6800 Trojan horses, 700 worms, and nearly 100 phishing URLs."

Learn more about Cisco's deployment of the Cisco IronPort S670 WSA at: www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/cisco_it_case_study_wsa_executive_summary.pdf.

[2] For additional tips on moving toward the BYOD model and to learn more about the five stages of Cisco's "Any Device" journey, see *Cisco Any Device: Planning a Productive, Secure, and Competitive Future*, www.cisco.com/en/US/solutions/collateral/ns170/ns896/white_paper_c11-681837.pdf.

drive it further. Rezai explains, “Executives are playing a lead role in driving adoption of BYOD in the enterprise. They’re taking the risk of embracing the chaos, but also saying, ‘We will do this systemically and architecturally, and evaluate our progress every step of the way.’” (See sidebar, “Questions to Ask Along Your Own ‘Any Device’ Journey,” on facing page.)

Governance also is critical to the success of a BYOD practice. Cisco, as an example, maintains a BYOD steering committee, which is led by IT but includes key stakeholders from other business units, such as human resources and legal. Without formal governance, companies cannot define a clear path for how to move the organization successfully and strategically from a managed world to an unmanaged or “borderless” world, where the security perimeter is no longer defined and IT does not manage every technology asset in use in the organization.

“Many people think BYOD is about the endpoint, but it’s much broader than that,” says Russell Rice, director of product management for Cisco. “It’s about ensuring consistency of the user experience working from any device, whether it’s in a wired or wireless environment or in the cloud. It’s about the policy elements of interaction. And it’s about your data, how it’s secured, and how it traverses inside all of those different environments. All of these things must be taken into account when moving to BYOD—it really is a change in mindset.”

Myth vs. **Reality**: Workers Won’t Accept Enterprise Control of Their Mobile Devices

Myth:
Employees will not accept an employer’s requirement to have some remote control over the personal mobile device that they want to use for both work and play.

Reality:
Enterprises and employees must find common ground, with the company recognizing the individual’s need to use the device of his or her choice and the worker understanding that the company must do whatever is necessary to enforce its security policy and stay in compliance with regulatory requirements related to data security.

Organizations must be able to identify unique devices when they enter the corporate network, link devices to specific users, and control the security posture of devices used to connect to corporate services. Technology is evolving that would allow the “containerization” of a device—that is, a virtual phone within a phone that could be shut off by an employer in the event the device is lost or stolen, without compromising a user’s personal data, which is kept separate. Within the next few years, viable security solutions based on this technology should be available for widespread enterprise use.

Until then, employees who want to use their personal device of choice for work must accept that the enterprise, for security reasons, retains certain rights in order to protect the device. This includes requiring, among other things:

- Passwords
- **Data encryption** (including device and removable media encryption)
- **Remote management options** that allow IT to remotely lock or wipe a device if it is lost, stolen, or otherwise compromised, or if the employee is terminated

If a worker does not accept policy enforcement and asset management requirements that are designed to elevate a mobile device’s status to “trusted” according to the enterprise’s security standards, then IT will not permit the employee to access safeguarded company assets with his or her device of choice.

Questions to Ask Along Your Own "Any Device" Journey

When Cisco first embarked on its "Any Device" journey, the company identified 13 critical business areas affected by this new paradigm. The table below highlights these focus areas and provides a list of questions that have helped Cisco identify—and avoid—potential pitfalls and determine how best to approach these considerations. Enterprises that want to adopt a BYOD practice should consider these questions as well.[3]

Business Area	Business Questions to Answer
Business continuity planning and disaster recovery	Should noncorporate devices be granted access or restricted from business continuity planning? Should there be an ability to remotely wipe any end device accessing the network if it is lost or stolen?
Host management (patching)	Will noncorporate devices be permitted to join existing corporate host-management streams?
Client configuration management and device security validation	How will device compliance to security protocols be validated and kept up to date?
Remote-access strategies	Who should be entitled to what services and platforms on which devices? Should a contingent worker be given the same entitlement to end devices, applications, and data?
Software licensing	Should policy change to permit installation of corporate-licensed software on noncorporate devices? Do existing software agreements account for users accessing the same software application through multiple devices?
Encryption requirements	Should noncorporate devices comply with existing disk-encryption requirements?
Authentication and authorization	Will noncorporate devices be expected or permitted to join existing Microsoft Active Directory models?
Regulatory compliance management	What will organizational policy be on the use of noncorporate devices in high-compliance or high-risk scenarios?
Accident management and investigations	How will corporate IT security and privacy manage incidents and investigations with noncorporate-owned devices?
Application interoperability	How will the organization handle application interoperability testing with noncorporate devices?
Asset management	Does the organization need to change how it identifies the devices it owns to also identify what it does not own?
Support	What will the organization's policies be for providing support to noncorporate-owned devices?

[3] Ibid.

Mobile Device Distribution in the Enterprise and Malware Encounters

The *Connected World* survey revealed that three out of four employees worldwide (77 percent) have multiple devices, such as a laptop and a smartphone or multiple phones and computers. Thirty-three percent of young professionals (one in three) say they use at least three devices for work. But which mobile device platforms are favored by most workers today, in general?

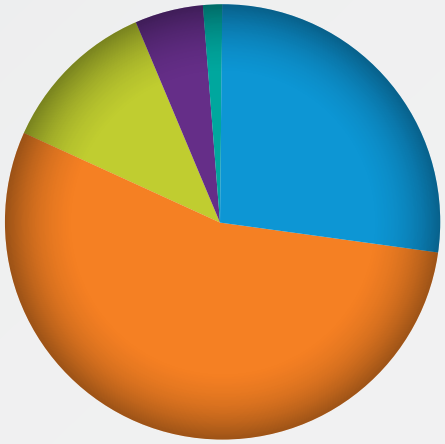
In conducting research for the latest *Cisco Global Threat Report,* Cisco ScanSafe took a close look at the types of mobile device platforms that workers around the world are using in the enterprise.* Surprisingly, RIM BlackBerry devices—which have long been accepted in most enterprise environments—are now the fourth most popular platform among workers.

Even more startling, perhaps, is that Apple Inc.'s iPhone, iPad, and iPod touch devices are currently the most dominant platform—significantly so. Google Android holds the second spot, with Nokia/Symbian devices ranking third.** These results underscore the powerful impact that consumerization of IT has had on enterprises in just a short period: The first iPhone was released in 2007; the first commercially available Android phone was launched in 2008.

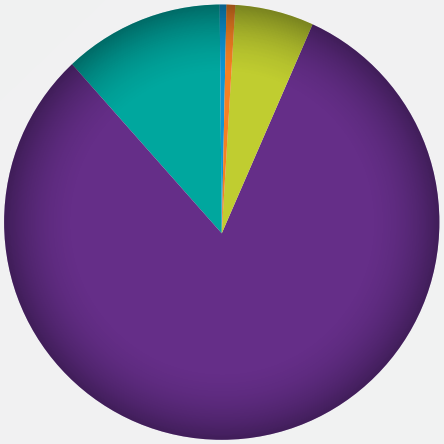
Cisco ScanSafe's research also provides insight into which mobile device platforms are encountering malware. The answer: all of them. (See chart below.) While BlackBerry devices are currently experiencing the majority of encounters (over 80 percent), Cisco's senior security threat researcher Mary Landesman says the malware is not targeted specifically at BlackBerry devices or users, and it's doubtful the malware encountered has infected or had any other impact on those devices.

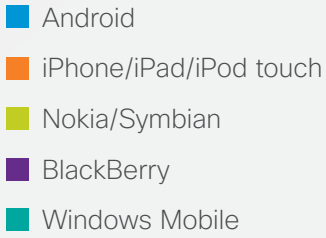
Landesman adds, "Wherever users go, cybercriminals will follow. As mobile device use continues to grow among enterprise users, malware targeting those devices—and thus, users—also will grow. (For more on cybercriminals' increasing investment in exploits that target mobile device users, see the "Cisco Cybercrime Return on Investment Matrix," page 26.)

Mobile Device Use by Enterprise



Normalized Distribution of Encounters





Source: Cisco ScanSafe

* Cisco ScanSafe processes billions of web requests daily. Survey results are based on an analysis of user agents normalized by customer count.
** Nokia/Symbian devices released as of October 2011.

The iPad Revolution: Tablets and Security

When the Apple iPad tablet computer launched in 2010, it was positioned (and embraced by the public) as a consumer device: Watching movies with the kids, browsing the web while sitting on the couch, and reading books were among the favorite use cases.

However, many industry sectors, like healthcare and manufacturing, quickly saw the appeal of a powerful, easy-to-use mobile device for business use that would bridge the gap between smartphones (too small) and laptops (too bulky). In a recent earnings call, Apple's chief financial officer said that 86 percent of Fortune 500 businesses and 47 percent of Global 500 companies are deploying or testing the iPad; companies such as General Electric Co. and SAP are creating custom iPad apps for internal processes; and Alaska Airlines and American Airlines pilots are using the iPad in cockpits to replace paper-based navigational information.[4]

At the same time, workers who use iPads and other tablets at home are asking their employers to let them use the devices at the office—yet another consumerization of IT milestone. This is reflected in the *Cisco Connected World* study, in which 81 percent of college students said they expect to be able to choose the device for their jobs, either receiving budget to buy devices of their choice, or bringing in their own personal devices.

Regardless of whether enterprises or workers are driving adoption of iPads and other tablets, the devices are generating questions and concerns about securing company information accessed via tablets. Unlike smartphones, iPads and tablets offer more robust compute platforms, with which workers can accomplish more than they can with smartphones. Forward-thinking enterprises want to enable the inclusion of tablets, without compromising security.

Innovation has caused constant change in IT—and the rate of change is increasing. Companies that design their device strategy around 2011's popular choice (in this case, the iPad) will have to start the clock on re-engineering their systems in a few years' time, when new vendors, products, and features emerge.

A more strategic decision is to shift the security conversation away from specific devices, and toward a BYOD enablement strategy with access based on user, role, and device type (for more on BYOD practice, see page 10). The key to enabling any device in the enterprise, whether it's company-owned or brought from home, is identity management—that is, understanding who's using the device, where they're using it, and what information they're accessing. In addition, enterprises welcoming tablet use in the workplace will need methods for device management (e.g., wiping data from lost devices), just as they have for smartphones and laptops.

For tablets—and indeed, whatever new-and-cool devices come into the enterprise next—security professionals need to preserve the user experience even as they add security features. For instance, iPad users love the device's touchscreen controls, such as moving fingers across the screen to view or zoom in on images. If IT departments build in security that restricts these much-loved features, users will balk at the changes.

"The best approach to tablet security is one that allows the ability to isolate business and personal apps and data reliably, applying appropriate security policy to each," says Horacio Zambrano, product manager for Cisco. "Policy happens in the cloud or with an intelligent network, while for the employee, their user experience is preserved and they can leverage the native app capabilities of the device."

[4] "Apple's corporate iPhone, iPad app strength bad news for rivals," ZDNet, July 20, 2011, www.zdnet.com/blog/btl/apples-corporate-iphone-ipad-app-strength-bad-news-for-rivals/52758.

The Influence of Mobile Devices, Cloud Services, and Social Media on Security Policy in the Enterprise

The cost of just one data breach can be staggering for an enterprise. Ponemon Institute estimates range anywhere from US$1 million to US$58 million.[5] The cost is not just financial, either: Damage to corporate reputation and loss of customers and market share are potential side effects of a high-profile data loss incident.

As more employees become mobile workers and use multiple devices to access company assets and rely on collaborative applications to work with others while outside the traditional "four walls" of the enterprise, the potential for data loss grows. As an example, the *Cisco Connected World* survey (www.cisco.com/en/US/netsol/ns1120/index.html) found that almost half (46 percent) of young professionals send work emails via personal accounts.

"The potential for data loss is high," says David Paschich, web security product manager for Cisco. "Enterprises are steadily losing control over who has access to their corporate network. And the simple fact that more employees are using mobile devices for work—and sometimes, multiple devices—means that the potential for data loss due to theft or loss of a device is greater."

Cybercriminals' growing preference toward the use of low-volume, targeted attacks, such as spearphishing campaigns (see "Global Spam Update: Dramatic Decline in Spam Volume", page 29), to steal information from high-value targets, and the increasing use of cloud-based file sharing services by enterprises to increase efficiency and reduce costs (see next section, "Securing Enterprise Data in the Cloud") are also heightening the potential for data to be stolen or compromised.

In this landscape, it's not surprising that more enterprises are renewing their focus on data loss prevention (DLP) efforts. "Today, businesses are evaluating their DLP programs to determine two things: if they are protecting the right data and if they are doing the right things to keep that data safe," says John N. Stewart, vice president and chief security officer for Cisco.

When categorizing data that must be kept safe, a good starting place for many organizations is to determine what data types require protection and security, based on applicable laws and regulations, which can vary by industry and geographic location (e.g., state, country). "You can't build rings of security around what you need to protect if you don't know what those things are," says Jeff Shipley, manager for Cisco Security Research and Operations. "This is a major shift in thinking for many organizations that focus their security controls on the systems and network, not the granularity of the actual data on the various systems, across multiple systems, or the network." He adds that enterprises should not overlook intellectual property when categorizing data to be secured.

Shipley also cautions enterprise IT departments not to miss obvious opportunities to prevent data from "walking out the front door." He says, "Here's an example: If an enterprise would protect its sensitive files, such as Excel sheets containing customer data, with controls to prevent downloading or moving the data from centralized applications or databases, the chance of an employee downloading that data to a personal or mobile device before leaving the company is greatly reduced."

Paschich also warns enterprises not to overlook a lower profile but very potent threat to data security—USB devices. "While companies are worrying about whether or not to let an employee connect to the network with an iPhone because they are concerned about undermining enterprise security, they are allowing their workers to plug USB devices into their laptops and copy whatever data they want."

He offers an additional tip for shoring up data protection in the enterprise: laying out DLP measures and acceptable use policies (AUPs) in separate documents. "These efforts are interlocking, certainly, but they are different," says Paschich. (See "The Future for Acceptable Use Policies," page19.)

Securing Enterprise Data in the Cloud

Cloud-based file sharing has become a popular and convenient method for sharing large files across the Internet, and it represents another potential risk area for enterprise data security. The idea of sensitive corporate information being passed back and forth among web-based cloud services—which are not managed by the enterprise—can cause sleepless nights for security professionals.

[5] *Email Attacks: This Time It's Personal*, Cisco, June 2011, www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf.

Cloud-based file sharing is gaining ground because it's easy to use: The signup process for services like Box.net or Dropbox is fast and simple, the services don't require hardware or advanced software, and they are free or low cost.

They also streamline collaboration between workers and external consultants and partners, since files can be shared without generating time-consuming and complex methods for accessing corporate networks. Younger workers, who are conditioned to rely on cloud services such as webmail and social networks, will no doubt embrace cloud file sharing and drive its greater adoption in the enterprise.

Ceding control of corporate data to the cloud, especially a piece of the cloud that an enterprise doesn't control, raises legitimate questions about information security. "Many new vendors in this market are startups with limited experience in providing enterprise-wide services, and with challenges it brings to the table," says Pat Calhoun, vice president and general manager of Cisco's Secure Network Services Business Unit. "In addition, security and encryption standards can vary widely from provider to provider. The benefits of file sharing in the cloud are many, but enterprises should ask tough questions of file sharing providers about their policies for maintaining security."

These questions include:

- What kind of encryption controls does the vendor provide?
- Which personnel have access to customer data?
- Who manages incident response and monitoring—the vendor or the customer?
- Does the vendor outsource some services to other suppliers? Are these suppliers caching data?
- Are DLP policies in place?
- Does the vendor conduct periodic security assessments?
- What redundancy measures are in place? How and where are backup files stored?

In tandem with assessing vendors, enterprises planning to establish corporate policy on file sharing in the cloud should take the following steps:

Establish a system for classifying data. Documents can be classified by their sensitivity level—for instance, "public," "confidential," "highly confidential," and so on, depending on business needs. Workers should be trained in how to apply these designations, and understand how they may affect the ability to share files in the cloud.

Establish a system for handling specialized data. Data that has legal or compliance implications needs special handling in terms of retention policies, physical location, and backup media requirements. Enterprises need to define policies around sending such data to external audiences, in addition to its classification per sensitivity levels.

Implement a DLP solution. File sharing vendors may not offer the granular level of DLP control that enterprises require. A DLP solution within the network can block data from being uploaded to file sharing services based on classifications—for instance, tax files or source code.

Provide identity management to control access. Users should be authenticated by the network before they are permitted to upload or download files. Leveraging corporate identity and identity federation for internal and external collaboration and managing the life cycle of provisioned accounts are key.

Set expectations from the vendor. Clear and well-defined policies and services should be part of the service level agreement (SLA)—for instance, redundancy systems and encryption controls, practices around access to data by third parties (e.g., law enforcement), defining shared responsibilities that might include incident response, monitoring and administrative functions, and data transfer/purging activities prior to termination of the contract.

U.S. Lawmakers Pursue Data Breach Disclosure Measures

Several high-profile data breaches in 2011, including incidents involving Sony Corp.[6] and Citigroup Inc.[7], have had U.S. lawmakers working to pass legislation that will impact how businesses protect consumer information and notify the public about cybersecurity incidents.

Three data breach and privacy bills were approved and passed by the U.S. Senate's Judiciary Committee in September 2011; the Senate Commerce Committee and the House Energy and Commerce Committee are working on versions as well. In the Senate, any version that passes likely will be a compromise of all versions that pass Senate committees and, perhaps, rolled into any larger comprehensive cyber bill that moves through the Senate. The versions that passed the Senate Judiciary Committee are:

The Data Breach Notification Act of 2011[8]
This measure would require federal agencies and businesses that "engage in interstate commerce" and possess data containing sensitive personally identifiable information to disclose any breaches.

The Personal Data Protection and Breach Accountability Act[9]
The act would establish a process to help companies create appropriate minimum security standards to safeguard sensitive consumer information. It also would require companies to issue prompt notification to individuals following a data breach.

The Personal Data Privacy and Security Act of 2011[10]
This measure would establish a national standard for companies to follow when reporting data breaches. Additionally, it would require businesses to implement data privacy and security programs designed to prevent data breaches from occurring. The bill also includes criminal penalties.

At the time reporting for the *Cisco 2011 Annual Security Report* was concluded, federal data breach notification legislation was still pending in the U.S. Congress, along with comprehensive cybersecurity legislation designed to help protect financial networks, transportation systems, and power grids. The Senate has been working on comprehensive cybersecurity legislation for over a year; in May 2011, the Obama administration shared its view of what such legislation should include.[11]

[6] "Sony Playstation Suffers Massive Data Breach," by Liana B. Baker and Jim Finkle, Reuters.com, April 26, 2011, www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.
[7] "Citi Says Many More Customers Had Data Stolen by Hackers," by Eric Dash, The New York Times, June 16, 2011, www.nytimes.com/2011/06/16/technology/16citi.html.
[8] The Data Breach Notification Act of 2011: www.govtrack.us/congress/billtext.xpd?bill=s112-1408.
[9] The Personal Data Protection and Breach Accountability Act: http://judiciary.senate.gov/legislation/upload/ALB11771-Blumenthal-Sub.pdf.
[10] The Personal Data Privacy and Security Act: www.govtrack.us/congress/billtext.xpd?bill=s112-1151.
[11] "Letters to House of Representatives and Senate on the Administration's cybersecurity proposal," WhiteHouse.gov, May 12, 2011, www.whitehouse.gov/sites/default/files/omb/legislative/letters/Cybersecurity-letters-to-congress-house-signed.pdf.

The Future for Acceptable Use Policies

Many acceptable use policies (AUPs) were born out of a need for enterprises to set down rules for how workers could access the Internet during work hours using corporate assets. Over time, many policies have become bloated catch-all documents designed to cover everything from Internet access to social media use to what employees cannot say about their company while engaging in online channels during off-hours. As a result, these policies, well intentioned as they are, have been difficult for employees to absorb and adhere to, and almost impossible for enterprises to enforce.

Given the results of the *Cisco Connected World* survey, it would appear that most AUPs are ineffective for another reason: Workers don't think they play a role in helping the enterprise to enforce such policies. The research reveals that three in five employees (61 percent) believe they're not responsible for protecting corporate information and devices; instead, their view is that IT and/or service providers are accountable. So the question is, what's the point of having an AUP?

"Acceptable use policies are important for many reasons, including for regulatory compliance, but most aren't realistic," says Gavin Reid, Cisco CSIRT manager. "Too many are long laundry lists filled with 'you-can't-do-this' items. They are really just a way for the enterprise to say to the employee, their legal department, or investigators, in the event of a security incident, 'Well, we said not to do that.'"

Reid says a better approach is for enterprises to rethink the AUP to make it relevant and enforceable, and adds that many organizations are already doing that. The new AUPs coming out of this process are leaner and stronger. They are generally much shorter lists—some include only a handful of items, such as making it clear that employees cannot use peer-to-peer (P2P) applications or send spam from their desktop. And every item on these lists is "technically enforceable," according to Reid, meaning that the organization has the technology in place to identify AUP violations.

"The current trend with AUPs is that businesses are taking a much more risk-based approach," says Nilesh Bhandari, product manager for Cisco. "Companies are honing in on what they absolutely must include in an AUP, and what makes the most sense for the business, especially in terms of time and cost required to monitor employees' adherence to the policy."

He adds that a well-defined AUP is easier for employees to understand and follow—and it gives the company greater leverage with its workforce. "Users will pay attention to an AUP when they fully understand what will happen if they fail to adhere to the policy," says Bhandari.

> "The current trend with AUPs is that businesses are taking a much more risk-based approach."
>
> —Nilesh Bhandari, product manager, Cisco

Myth vs. **Reality**: AUPs Cannot Be Enforced

Myth:
AUPs have no impact because they cannot be enforced—and they are simply too difficult for the enterprise to create in the first place.

Reality:
Organizations cannot effectively enforce catch-all policies. While it does take time and research to determine what an AUP should include and whether or not each item truly can be enforced, the end result will be a policy that is easier for employees to understand and follow—and that is more likely to enhance enterprise security.

Special focus should be given to educating employees on safe use of email and the web, as these are avenues cybercriminals typically take to infiltrate and infect networks, steal intellectual property and other sensitive data, and compromise individual users.

Getting Started with Collaboration Security

Enterprises can use the following steps to help establish security policies, technologies, and processes related to collaboration and social media security:

- **Create a business plan for collaboration** and social networking solutions, starting with the business need.
- **Craft clear security governance mechanisms** for collaboration.
- **Create policies on information confidentiality** and expectations for employee activity when interacting on collaboration sites.
- **Define policies on network security measures**, such as remote access by mobile devices, level of password protection, and use of direct file sharing.
- **Identify regulatory and compliance requirements** that might restrict use of or information disclosure on social media.
- **Create training resources for all users.**

Social Media: Policies Paired with Technology Controls

Judging from the results of the *Connected World* study, college students and young professionals are likely to find ways around restrictions on social media access if it suits their needs—regardless of corporate policies. Three in four employees surveyed believe their companies should allow them to access social media and personal sites with their work-issued devices.

Additionally, 40 percent of college students said they would break a company's social media rules. That's a significant slice of the potential workforce surveyed in this study—and it serves as a warning to enterprises as they grapple with their AUPs for social media. In other words, you can ban or restrict social media, but odds are good that your employees will access it anyway.

Organizations with AUPs that put a stranglehold on social media access for employees will likely find it hard to attract the best and the brightest young talent. Twenty-nine percent of students surveyed said they would decline a job offer from a company that did not allow them to access social media during working hours. And of those students who would accept such a job, only 30 percent said they would abide by the stated policies.

"Access to social media and technology freedom of choice will become make-or-break benefits for younger workers considering where to start their careers," says Chris Young, senior vice president for the Security Group at Cisco. "HR organizations need to account for these factors in corporate culture and policy to retain a competitive edge. Enterprises should define a realistic compromise between the desires of employees to share and the business requirements of maintaining IT security, data, privacy, and asset protection."

Such a compromise involves granting access to social media and other collaboration technologies while using technology controls to deflect threats such as malware or phishing messages. In most cases, the security settings in social networks are controlled by users, not by IT. To compensate for this lack of control, additional security measures can be implemented—for instance, an intrusion prevention system to protect against network threats, and reputation filtering to detect suspicious activity and content.

Technology controls should be paired with user training that clarifies the enterprise's expectations for appropriate behavior and practices while accessing social media on company devices or via company networks. As discussed earlier (see "Social Media: Now, It's a Productivity Tool," page 8), young professionals have become so comfortable sharing information in the social media environment that they may not realize—nor have they ever been taught—that even small pieces of information posted on a social network can cause damage to a business. Lack of both user training about collaboration security concerns and guidelines for disclosing information online can be causes for this risk exposure.

PART 2

Cyber Threat Outlook for 2012: The Hacktivism Factor

Today's enterprises are grappling with an array of security issues brought about by changing attitudes and work habits among their employees, and the dynamics of a more collaborative, connected, and mobile world. As this half of the *Cisco 2011 Annual Security Report* will examine, enterprises also must continue to protect against a wide range of potent threats that cybercriminals are already reaping rewards from, and are investing additional resources in refining—among them are advanced persistent threats (APTs), data theft Trojans, and web exploits.

However, enterprises now must consider another potential security threat that could be even more disruptive to their operations if they were to be targeted: hacktivism.

"Hacktivism is a morph of traditional hacking," says John N. Stewart, vice president and chief security officer for Cisco. "Hackers used to hack for fun and notoriety. Then, it was for a prize or monetary gain. Now, it's often about sending a message, and you may never know what made you a target. We're defending a new domain now."

Hacktivism—a blend of hacking and activism—catapulted to the top tier of security concerns in late 2010 when supporters of WikiLeaks.org launched distributed denial of service (DDoS) attacks against institutions such as PayPal and MasterCard; the initiative was dubbed "Operation Payback."[12] In many ways, hacktivism is a natural extension of how people are using the Internet today—to connect with like-minded people all over the globe. The Internet serves as a powerful platform for those who want to make a statement and grab the attention of a wide audience, and motivate others to pursue similar actions. (See "Social Media Wields 'Gathering' Power," on opposite page.)

Behind Operation Payback was a group known as the Anonymous collective, which has been growing in both membership and influence worldwide ever since. (For more on Anonymous, see the "Cisco Cybercrime Showcase," on page 24.) Most recently, Anonymous has been connected to the Occupy Wall Street movement.[13] The "Occupy" protests began in New York City, but quickly spawned similar gatherings in more than 900 cities around the world. Activists representing the Anonymous collective have encouraged members to participate in the movement, which generally has been peaceful, but has led to violent clashes with law enforcement in some cities, including Rome, Italy,[14] and Oakland, California.[15] At times, factions of Anonymous that identify with the Occupy movement have threatened greater disruption, such as hacking campaigns to halt the operations of major financial exchanges.

Incidents of hacktivism by other groups in the last year have helped to elevate this threat to the top tier of cyber threat concerns for enterprises. LulzSec, for example, focused its efforts on law enforcement organizations, executing DDoS attacks and data theft against a U.K. cybercrime organization and Arizona law enforcement.[16] In July, a related group, known as "Script Kiddies," hacked Fox News Twitter accounts to post that U.S. President Barack Obama had been assassinated.[17]

Hacktivism can happen quickly and without warning—although Anonymous did announce some of its intended targets, such as HBGary Federal, a firm hired by the U.S. federal government to track down cyberactivists targeting organizations that had pulled support from WikiLeaks.org. While the threat of hacktivism may seem remote, it's very real, and represents a shift in the nature of cybercrime itself.

"Understanding criminal motivation has been a guiding principle in charting security strategy. However, the hacktivists' goal of mayhem undermines this model, as any enterprise can be targeted at any time for any reason by anybody," explains Patrick Peterson, senior security researcher for Cisco. "What an enterprise would try to protect from being compromised in a 'traditional' security breach, such as intellectual property, may be of no interest to this type of hacker. The 'value' derived from the action is when the hacker can disrupt, embarrass, or make an example of their target—or all of the above."

Stewart adds, "Planning ahead for an incident of hacktivism means creating a clear action plan that outlines what the organization would say and do *after* an event has occurred. Developing this plan should be a cross-functional effort that includes management, security teams, legal, and even communications professionals. If this happens to your business, handle it well, as it can result in lasting damage to your brand. As is true with many things, be prepared and have your game plan in place before an incident occurs."

[12] "'Anonymous' Launches DDoS Attacks Against WikiLeaks Foes," by Leslie Horn, PCMag.com, December 8, 2010, www.pcmag.com/article2/0,2817,2374023,00.asp#fbid=jU1HvGyTz7f.
[13] Occupy Wall Street website: http://occupywallst.org/.
[14] "Occupy protests spread around the world; 70 injured in Rome," by Faith Karimi and Joe Sterling, CNN.com, October 15, 2011, www.cnn.com/2011/10/15/world/occupy-goes-global/index.html.
[15] "Occupy Oakland Violence: Peaceful Occupy Protests Degenerate Into Chaos," Associated Press, The Huffington Post, November 3, 2011, www.huffingtonpost.com/2011/11/03/occupy-oakland-violence-_n_1073325.html.
[16] "LulzSec Releases Arizona Law Enforcement Data, Claims Retaliation for Immigration Law," by Alexia Tsotsis, TechCrunch.com, June 23, 2011, http://techcrunch.com/2011/06/23/lulzsec-releases-arizona-law-enforcement-data-in-retaliation-for-immigration-law/.
[17] "Script Kiddies Hack Fox News Account, Tweet Obama's Death," by Nicholas Jackson, The Atlantic, July 4, 2011, www.theatlantic.com/technology/archive/2011/07/script-kiddies-hack-fox-news-account-tweet-obamas-death/241393/.

Geopolitical Trends: Social Media Wields "Gathering" Power

If anyone still needed evidence that social media can spark social change at lightning speed, 2011 was the year that this power was proven. The "Arab Spring" protests early in the year, and the riots in London and other British cities during the summer, showed that social media disseminates calls to action like no other medium before it. In both cases, Twitter and Facebook were used to drive attendance at public gatherings—and, also in both cases, government entities suggested blocking access to social media by cutting off Internet access or seizing personal account records.

A September 2011 University of Washington study found that social media, especially Twitter, "played a central role in shaping political debates in the Arab Spring," particularly in Egypt and Tunisia, according to the study's summary. "Conversations about revolution often preceded major events on the ground, and social media carried inspiring stories of protest across international borders."[18] Social media watchers expect this trend to continue, as anti-government frustration finds a voice in social media networks.[19]

The implications for enterprises and for their security lie in the possibility of social media being used to cause upheaval within their own organizations or toward their brands or industries. (See "Cyber Threat Outlook for 2012: The Hacktivism Factor," page 22.) "The perception of anonymity online increases the risk of unintended consequences if so-called netizens feel at liberty to lay blame but skip fact-checking," says Cisco global threat analyst Jean Gordon Kocienda. "For companies and corporate executives, particularly in the current global environment of frustration toward perceived privileged groups, this increases both physical and virtual security concerns."

In addition, enterprises can expect to undergo serious business disruption if offices or employees are based in areas undergoing such upheaval—for instance, lack of Internet access if local authorities shut it down as a security measure. It's also possible organizations seen as aiding or abetting a corrupt regime could be targeted, or could suffer a backlash if they are viewed as trying to stifle a revolutionary movement.

Also on enterprises' radar is the increasing tendency of government organizations to seek to block social media or even Internet service on a broad scale, or request access to social media account or mobile device information that is normally private. For example, during the riots in the United Kingdom, people used BlackBerry Messenger (BBM), the instant messaging service for BlackBerry users, to trade information about sites to loot, or where protestors should gather. BBM is encrypted phone-to-phone messaging that, generally speaking, is harder for law enforcement authorities to trace. RIM, BlackBerry's creator, agreed to cooperate with U.K. police teams trying to identify BBM users who advocated riots or looting, although the company did not say what type of BBM account information it would disclose.[20]

In the aftermath of the riots, British officials warned that, in the future, the government might request extended police powers to curb unrest, and proposed asking social media providers to restrict access to their services during such emergency situations.

Twitter responded by pointing to a blog post from earlier in 2011 affirming the company's commitment to keeping the service up and running no matter what world-shaking events were being discussed via tweets: "We don't always agree with the things people choose to tweet, but we keep the information flowing irrespective of any view we may have about the content."[21]

Security watchers anticipate a tug-of-war between governments—which will increasingly demand access to user data in order to maintain law and order—and privacy advocates, who will protest any such disclosures from technology providers. As an example, India has expressed concern over its ability to access such data (for instance, to track terrorist activity), and has made an agreement with RIM that the government can request the company's private user data on a case-by-case basis. The European Data Retention Directive, which was created in 2006 and calls for communications data to be retained in case it is needed by law enforcement authorities, has been implemented by some countries in the European Union, yet delayed by others.[22]

"What is clear is that governments globally are struggling to apply the new facts of technology and communications to the underlying principles of law and society," says Adam Golodner, director of global security and technology policy for Cisco. "This has always been the case as technology moves forward, and in cyber, this application of the new facts to the old principles will be the core policy issue for the foreseeable future."

[18] "Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?," Project on Information Technology and Political Islam, http://pitpi.org/index.php/2011/09/11/opening-closed-regimes-what-was-the-role-of-social-media-during-the-arab-spring/.
[19] "U.K. social media controls point to wider 'info war'," by Peter Apps, Reuters, August 18, 2011, www.reuters.com/article/2011/08/18/us-britain-socialmedia-idUSTRE77H61Y20110818.
[20] "London Rioters' Unrequited Love For BlackBerry," by Nidhi Subbaraman, FastCompany.com, August 8, 2011, www.fastcompany.com/1772171/london-protestors-unrequited-love-for-blackberry.
[21] "The Tweets Must Flow," Twitter blog, January 28, 2011, http://blog.twitter.com/2011/01/tweets-must-flow.html.
[22] "Sweden postpones EU data retention directive, faces court, fines," by Jan Libbenga, The Register, March 18, 2011, www.theregister.co.uk/2011/03/18/sweden_postpones_eu_data_retention_directive/.

Announcing the 2011 Winners of the Cisco Cybercrime Showcase

There will always be villains and heroes, and the security industry is no exception. The cast of characters may change, but every year, malicious actors are doing their best to identify new ways to steal money and information and cause mayhem through online channels—and cybercrime fighters are working tirelessly to thwart them. In this, the third annual Cisco Cybercrime Showcase, we once again recognize representatives from both the "good side" and "bad side" of the security battlefield who have had a notable impact on the cybersecurity landscape, for better and for worse, in the past year.

[23] "Deactivating botnets to create a safer, more trusted Internet," Microsoft.com: www.microsoft.com/mscorp/twc/endtoendtrust/vision/botnet.aspx.

[24] "Rustock take-down proves botnets can be crippled, says Microsoft," Computerworld.com, July 5, 2011, www.computerworld.com/s/article/9218180/Rustock_take_down_proves_botnets_can_be_crippled_says_Microsoft.

[25] "How Microsoft Took Down Massive Kelihos Botnet," The Huffington Post, October 3, 2011, www.huffingtonpost.com/2011/10/03/microsoft-kelihos-botnet_n_992030.html.

THE GOOD
MICROSOFT

Microsoft's technology has always attracted the attention of criminals because of its pervasiveness in the enterprise and among consumers. In particular, botnet owners have exploited the Windows operating system using social engineering, web-based attacks, and unpatched vulnerabilities. In recent years, Microsoft has fought back against botnets in three big ways.

First, Microsoft has dramatically improved product security. Key developments include aggressive vulnerability discovery and weekly patch cycles; implementation of Microsoft Security Development Lifecycle (SDL) to dramatically increase product security; auto-update systems for all of Microsoft's software products; significant changes to Windows Internet Explorer, including a new security model for ActiveX controls; and development of the Malicious Software Removal Tool (MSRT), which surgically removes malware from PCs. MSRT has been deployed against malware families powering more than 150 of the world's largest botnets, including Zeus (Zbot), Cutwail, Waledac and Koobface, to remove hundreds of millions of PC malware infections. Cisco research has shown massive declines year over year in web exploit toolkits' successful exploitation of Microsoft technologies.

Second, Microsoft has led the security community in the fight against cybercrime. Microsoft's Digital Crimes Unit hosts the annual Digital Crimes Consortium (DCC), which provides an opportunity for law enforcement officials and members of the technology security community to discuss enforcement efforts involving cybercrime worldwide. This year's event included 340 attendees from 33 countries.

Third, Microsoft has aggressively pursued legal actions against cybercriminals. In 2010, Microsoft took legal action to shut down the Waledac botnet—which had infected hundreds of thousands of computers worldwide and was sending as many as 1.5 billion spam messages daily—by asking a federal judge to file a restraining order against almost 300 Internet domains believed to be controlled by Waledac-related criminals. This action cut off communications between the botnet's command-and-control centers and its compromised computers, effectively "killing" the botnet.[23]

In early 2011, Microsoft lawyers and U.S. marshals seized command-and-control servers for the Rustock botnet, which were housed at several web-hosting providers across the United States. Malware promulgated by Rustock, which was operated by Russian criminals and mostly delivered fake pharmaceuticals spam, dropped dramatically, and the botnet's activity slowed to a halt. Additionally, Microsoft offered a US$250,000 reward for information leading to the arrest of Rustock's creators.[24] According to the Cisco IronPort SenderBase Security Network, since Rustock has been sidelined, daily spam volume worldwide has dropped dramatically.

In September 2011, Microsoft used similar legal tactics to shut down the Kelihos botnet—and in legal filings actually named a defendant for the first time, calling out the alleged owner of the web domain controlling the botnet.[25]

Microsoft's anti-botnet actions—combined with the company's record numbers of vulnerability patch releases, which also help clamp down on criminal activity—have turned it into a cybercrime crusader. The company's Project MARS (Microsoft Active Response for Security), which oversees these botnet takedown efforts, also has shared its findings about botnets with members of the security industry.

THE BAD

ANONYMOUS

Anonymous, described as a "decentralized online community acting anonymously in a coordinated manner," is a "loose coalition of Internet denizens" that has been around for several years, but making headlines more often lately as the group becomes increasingly associated with collaborative, international hacktivism. (For more on hacktivism, see "Cyber Threat Outlook for 2012: The Hacktivism Factor," page 22.)

Those who identify with the Anonymous collective are located all over the world and connect with one another through Internet forums, imageboards, and other web-based venues such as 4chan, 711chan, Encyclopedia Dramatica, IRC channels, and even mainstream sites such as YouTube and Facebook. "This is a group that is fairly well organized, yet loosely affiliated," says Patrick Peterson, senior security researcher for Cisco. "The people involved are highly talented–and incredibly ambitious. In many cases, their actions are not motivated by profit. It's more a case of 'Look what I can do.' And when they're done, they disassemble and disappear as quickly as they came together."

In 2011, Anonymous has been associated with a number of high-profile hacking incidents, some announced in advance and all intended to make a statement, including direct attacks on the websites of:

- Numerous U.S. law enforcement organizations, which resulted in the release of peace officer and confidential informant personal information
- The government of Tunisia, as part of the "Arab Spring" movement (see "Social Media Wields 'Gathering' Power," page 23)
- Security firm HBGary Federal
- Sony Computer Entertainment America

What threat does Anonymous pose moving forward? "This group has the ability to inflict real damage," says Scott Olechowski, threat research manager for Cisco. "Most of what we've seen from them so far hasn't been too extreme–arguably, more disruption than the actual damage they are capable of. You could define them as mischievous right now. But if you add some people into the Anonymous mix who truly want to cause damage–or if the group takes things one step too far when trying to make a statement–there could be a real problem."

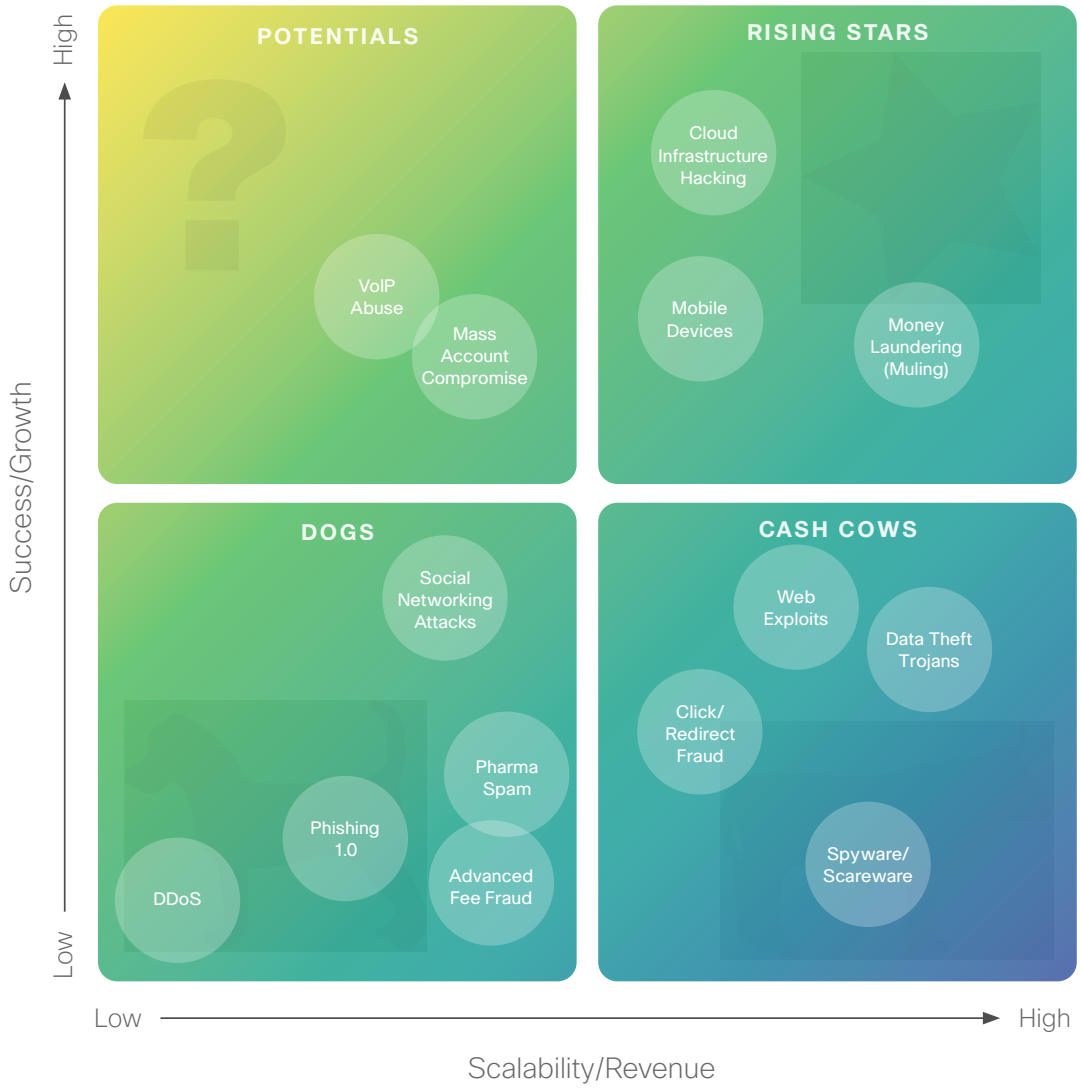
Consider this almost-incident that had the potential to send shockwaves through an already uncertain global economy: In October, factions of Anonymous aimed big by threatening to "erase" the New York Stock Exchange on October 10, 2011, through a distributed DDoS attack in a show of support for the Occupy Wall Street movement.[26] One possible reason the group did not carry through with its promise to bring down the exchange is because "the rallying cry drew out criticism from supporters and detractors alike, with most decrying the effort."[27] So it would appear that Anonymous, loosely connected as it is right now, can be influenced by its collective conscience not to inflict serious damage–at least, in this case.

> "The people involved are highly talented – and incredibly ambitious. In many cases, their actions are not motivated by profit. It's more a case of 'Look what I can do.'"
>
> –Patrick Peterson, senior security researcher, Cisco

[26] "'Anonymous' Hackers Group Threat to New York Stock Exchange," by Ned Potter, ABC News, October 10, 2011, http://abcnews.go.com/Technology/anonymous-hackers-threaten-erase-york-stock-exchange-site/story?id=14705072.

[27] "Blink and You Missed It: Anonymous Attacks NYSE," by Chris Barth, Forbes.com, October 10, 2011, www.forbes.com/sites/chrisbarth/2011/10/10/blink-and-you-missed-it-anonymous-attacks-nyse/.

The Cisco Cybercrime Return on Investment (CROI) Matrix



The Cisco CROI Matrix predicts cybercrime techniques that will be "winners" and "losers" in 2012.

The Cisco CROI Matrix tracks the performance of financially motivated cybercrime operations, which increasingly are managed and organized in ways similar to sophisticated, legitimate businesses. This matrix specifically highlights the types of aggressive actions Cisco security experts predict cybercriminals are likely to focus most of their resources toward developing, refining, and deploying in the year ahead.

Potentials: Mass Account Compromise, a newcomer to this year's Cisco CROI Matrix, essentially involves cybercriminals "making use of table scraps left from data theft," according to Patrick Peterson, senior security researcher for Cisco. They piece together information gathered from data theft Trojans to extract low-value username/password credentials. The credentials are then used as "stepping stones" to find credential reuse on a valuable online banking site, or to use webmail credentials to spy on a victim's personal email in order to lay groundwork for a more aggressive action. "Cybercriminals are looking at the tons and tons of information they're collecting in a different way. They're now thinking, 'Could this webmail or dating site username/password I have be the skeleton key to a high-value account? Or could it be a stepping stone for a webmail exploit that will allow me to do other things, like password resets and reconnaissance, that could lead to even bigger prizes?" says Peterson.

Cybercriminals are also accelerating investment in VoIP and other telephony abuse techniques. As reported in the *Cisco 2010 Annual Security Report*, many miscreants already have found success in targeting small or midsize businesses with this technique, causing significant financial losses for some organizations. VoIP Abuse, which was listed as a "Potential" on last year's matrix, involves the hacking of private branch exchange (PBX) systems. VoIP abusers place fraudulent, long-distance calls—usually international calls. Some criminals use VoIP systems for more sophisticated "vishing" scams (telephone-based phishing), designed to collect sensitive information from users, such as Social Security numbers. Caller ID spoofing attacks against phone-based verification systems are also on the rise.

Rising Stars: Money Laundering (Muling) is expected to remain a key focus area for cybercrime investment in 2012. Discussed in detail in the *Cisco 2010 Annual Security Report*, criminals leveraging data theft malware have access to numerous online bank accounts but face a bottleneck in extracting funds safely overseas without leaving a direct trail.[28] Money mules provide this solution. Muling operations have become increasingly elaborate and international in scope recently with some of the best data coming from "Operation Trident Breach," the arrest of more than 60 cybercriminals who successfully stole US$70 million using money mules.[29] While it is estimated that only one in three money mule transactions are successful–and money mules are easy to arrest, at least in the United States–mule networks continue to grow as real criminals have plenty of bank accounts and mules to burn.

A not-so-surprising newcomer among the "Rising Stars" is Mobile Devices, which was listed in the "Potentials" category in the 2010 matrix. Cybercriminals, as a rule, focus their attention on where the users are, and increasingly, people are accessing the Internet, email, and corporate networks via powerful mobile devices. Mobile device attacks have been around for years now, but historically have not been widespread, and were more akin to research projects than successful cybercrime businesses. But that's changing–fast.

Mobile campaigns not only are becoming more prevalent, but also, successful–and therefore, important to cybercriminals. New mobile OS platforms present new security vulnerabilities to exploit. Many cybercriminals are reaping rewards with fake mobile applications that serve up malware. And with mobile devices quickly replacing traditional PCs as business computing tools, cybercriminals are investing more resources in developing APTs to exploit two-factor authorization and help them gain access to corporate networks where they can steal data and/or conduct "reconnaissance missions."

Meanwhile, as more businesses embrace cloud computing and hosted services, cybercriminals are also looking to the cloud in search of moneymaking opportunities with Cloud Infrastructure Hacking. "Criminals see the potential to get more return on their investment with cloud attacks," says Scott Olechowski, threat research manager for Cisco. "Why focus all your efforts on hacking into one enterprise when you can compromise hosted infrastructure and potentially access information belonging to hundreds or even thousands of companies?"

Olechowski adds that recent data security incidents–such as hackers gaining access to customer names and email addresses stored in the systems of email marketer Epsilon Data Management LLC[30]–underscore the growing trend toward "hack one to hack them all."

Cash Cows: Two of 2010's "Rising Stars"–Data Theft Trojans and Web Exploits–have made their way to the 2011 "Cash Cows" category, as they are now among the favorite money-makers for cybercriminals. But this move isn't just because criminals have perfected their skills with these techniques; the prevalence of cheap and easy-to-use web exploit toolkits and data theft Trojan exploits means anyone who wants to get into the game can do so with relatively little effort or investment. Other old favorites such as Spyware/Scareware and Click/Redirect Fraud have lost a little luster, but maintained their role as loyal workhorses for cybercriminals during 2011–and will continue to do so in 2012.

Dogs: Two new entrants to the "Dogs" category are Pharma Spam and Advanced Fee Fraud. Pharma spam, a "Cash Cow" in the 2010 Cisco CROI Matrix, has fallen out of favor due to law enforcement activities and botnet shutdowns. (See the Cisco Cybercrime Showcase, "The Good: Microsoft," page 24.) Numerous pharma spam criminals have been arrested or have gone underground to avoid capture, including Igor Gusev of SpamIt/Glavmed; Pavel Vrublevsky of RX-Promotions/Eva Pharmacy; Oleg Nikolaenko, operator of the massive Mega-D botnet; Georg Avanesov, operator of the Bredolab botnet; and many others. With so many of the once-massive botnets such as Waledac, Mariposa, Cutwail (reportedly the largest botnet ever), Rustock, Bredolab, and Mega-D either long gone or severely crippled, and authorities more vigilantly scanning the horizon for prolific spammers, pushing out pharma spam simply does not generate the returns it used to for cybercriminals.[31]

Meanwhile, another "Cash Cow" from last year, Advanced Fee Fraud, is now making its way toward the exit door. Today's users are simply better educated–and spam filters are better tuned–which means this technique is no longer delivering significant returns to cybercriminal operations. The labor-intensive "Nigerian prince" scam still runs, but profits continue to decline.

Old dogs still hanging around on the matrix are Phishing 1.0 scams and DDoS attacks. Social Networking Attacks continue to take a backseat as users become even savvier about navigating the online "Social Sphere." Many more users are now instinctively less trusting of others they don't know who try to interact with them on social networks. They also are taking advantage of privacy controls from their social network providers, and generally, being less open when sharing personal information on these sites. Social networking attacks will not fade away completely, but sophisticated cybercriminals are unlikely to continue investing their resources in refining or expanding such exploits. Making these types of scams work has simply become too labor-intensive and time-consuming, especially now that many in the shadow economy are making a specific effort to be more strategic when investing their resources.

[28] Cisco 2010 Annual Security Report, www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf.
[29] "Ukraine Detains 5 individuals Tied to $70 million in U.S. eBanking Heists," Brian Krebs, Krebs on Security blog, October 2, 2010, http://krebsonsecurity.com/tag/operation-trident-breach/.
[30] "Breach Brings Scrutiny: Incident Sparks Concern Over Outsourcing of Email Marketing," by Ben Worth, The Wall Street Journal, April 5, 2011, http://online.wsj.com/article/SB10001424052748704587004576245131531712342.html.
[31] For more on the takedown of these botnets, see the Cisco 2010 Annual Security Report, www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf.

2011 Vulnerability and Threat Analysis

The *Cisco Annual Security Report* provides a comparison of the rise and fall of vulnerabilities and threats by category, as well as the estimated impact of these exploits.

The **Vulnerability and Threat Categories** chart below shows a slight increase in recorded vulnerabilities and threats—a significant trend, since they generally have been on the decline since 2008. One factor causing the increase is vulnerabilities in major software vendors' open source packages or code, such as those using the open source browser engine WebKit. A single vulnerability in an open source product like WebKit can impact multiple major products and result in multiple advisories, updates, and patches. Apple continued to release large updates this year for several of its products, relating to the inclusion of open source software.

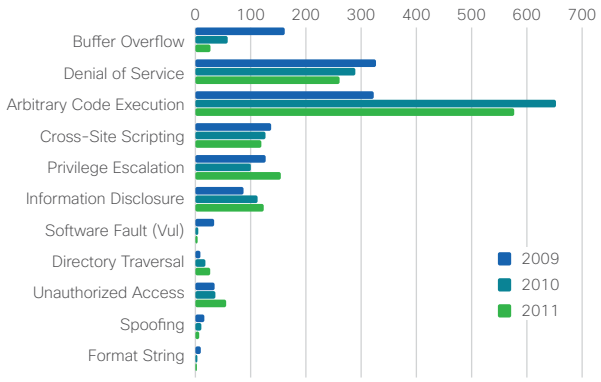
Going into 2012, security experts are watching vulnerabilities in industrial control systems and supervisory control and data acquisition systems, also known as ICS/SCADA systems. These systems present a growing area of concern, and government cyber defense initiatives are focused on addressing these vulnerabilities. As reported in the *Cisco 2010 Annual Security Report*, the Stuxnet network worm was designed to infect and tamper with these systems.

The good news for 2011 is a decline in basic coding errors: buffer overflows, denial of service, arbitrary code execution, and format string vulnerabilities. However, this does not include vulnerabilities and corrections related to flaws that allow SQL injection attacks, which continue to be a widespread problem.

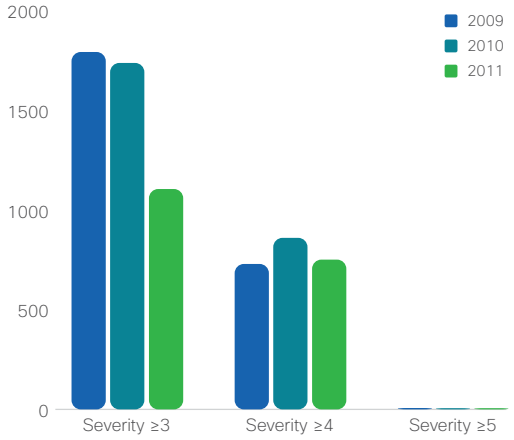
The Cisco IntelliShield Alert Severity Ratings reflect the impact level of successful vulnerability exploits. In 2011, severity levels continued along a slight decline evident since 2009, which mirrors recent declines in vulnerabilities and threats. Moving forward into 2012, severity levels are expected to remain at current levels, with no widespread attacks or exploits of specific vulnerabilities.

Cisco IntelliShield Alert Urgency Ratings reflect the level of threat activity related to specific vulnerabilities. 2011 is notable for a significant spike in Urgency 3, meaning a limited number of exploits were detected, but additional exploits still could be possible. This increase indicates that while there are a greater number of active threats in circulation on the Internet, they generally do not rise to the level of

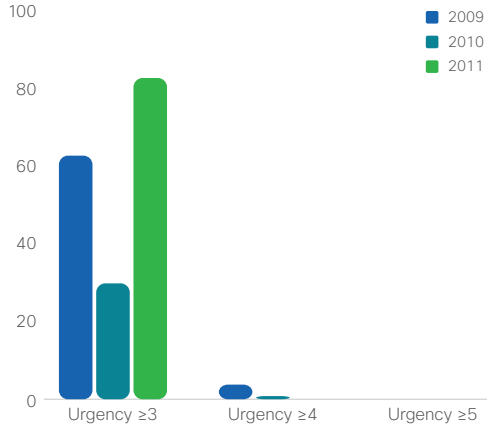
Vulnerability and Threat Categories



Cisco IntelliShield Alert Severity Ratings



Cisco IntelliShield Alert Urgency Ratings



Urgency 4 (several incidents of exploitation have been reported across a variety of sources) or Urgency 5 alerts (widespread incidents of exploitation have been reported across a variety of sources, and exploits are easy to perform).

Threats and exploits also are more narrowly focused, as opposed to widespread exploits involving Internet worms and malicious code. The threats tend to be associated with attack toolkits, which assist in launching attacks using individual vulnerabilities on individual systems.

As discussed in the *Cisco 2010 Annual Security Report*, large botnets such as Zeus—which commandeered as many as 2 million to 3 million computers worldwide—have been used to steal banking information and login data for years. Recently, botnet creators have launched attack toolkits, in which botnet code is built in, enabling the creation of a host of smaller botnets.

Instead of just a few very large botnets, usually managed by established criminal enterprises, there are now dozens of smaller botnets engaging in criminal activity. "When there were only a few large botnets in existence, it was easier to track them and understand how they operated," says Jeff Shipley, manager for Cisco Security Research and Operations. "The availability of botnet toolkits has greatly increased the number of botnets, allowed more variations, and complicates the task of analyzing their behavior patterns and providing protection from them."

The new smaller botnets still aim to gather bank account information, as the larger Zeus botnets do. However, the number and variety of these smaller botnets make it challenging for security professionals to track their movements.

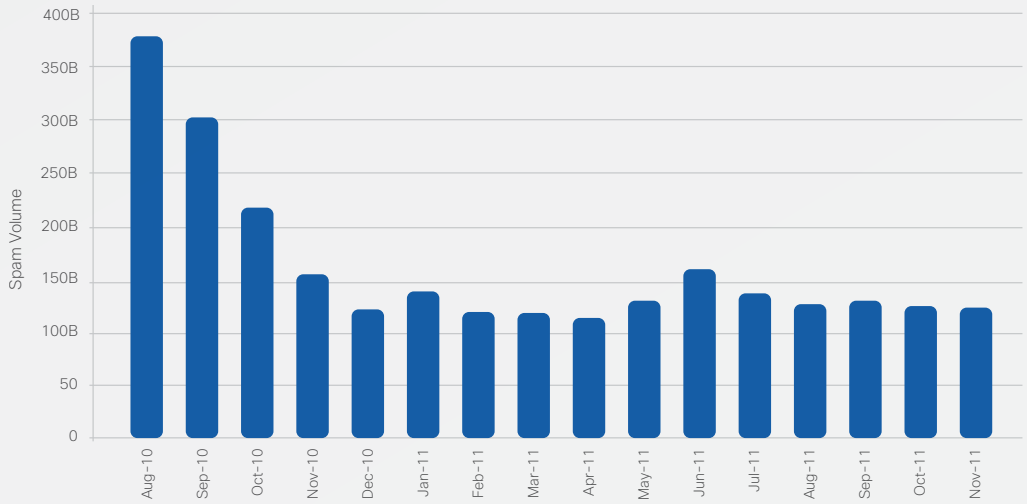
Global Spam Update: Dramatic Decline in Spam Volume

Thanks to criminals' preference for targeted campaigns, spam does not appear to be as lucrative as it used to be. According to Cisco Security Intelligence Operations (SIO), spam volume dropped from more than 379 billion messages daily to about 124 billion messages daily between August 2010 and November 2011—levels not seen since 2007.

Before 2011, some cybercriminals had already started to shift their focus toward more targeted attacks, using their resources to reach out to specific people in an organization (such as financial or IT personnel) with a scam message designed to obtain sensitive network login data or other account information. Targeted scams need only a single response from a recipient to be considered successful, whereas mass spam campaigns require a much higher response rate to be profitable.

But events over the past year have disrupted traditional spammers' business models so significantly that many have been forced to channel their resources toward developing targeted attacks. Beginning in 2010 and continuing into 2011, law enforcement authorities and security organizations around the world have been working closely together to shut down or severely limit the activity of some of the biggest spam-sending botnets. SpamIt, a large spam-sending affiliate network, closed down in 2010 after Russian police pressed charges against its owner. In addition, major botnets were crippled or shut down, including Rustock, Bredolab, and Mega-D.

The impact on the business of cybercrime is significant: Cisco SIO estimates that the cyber-criminal benefit resulting from traditional mass email-based attacks declined more than 50 percent (on an annualized basis) from June 2010 to June 2011—from US$1.1 billion to US$500 million.[32]



Source: Cisco SIO

[32] *Email Attacks: This Time It's Personal*, Cisco, June 2011, www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf.

Spam Volume by Country: 2011 Highlights

Cisco SIO also tracks spam volume originating from countries worldwide. As of September 2011, India had the highest percentage of spam volume (13.9 percent). In 2010, the country ranked second in spam volume, behind the United States, which saw its spam volume drop dramatically from January to September 2011, from 10.1 percent to 3.2 percent. The United States now ranks ninth in total spam volume worldwide.

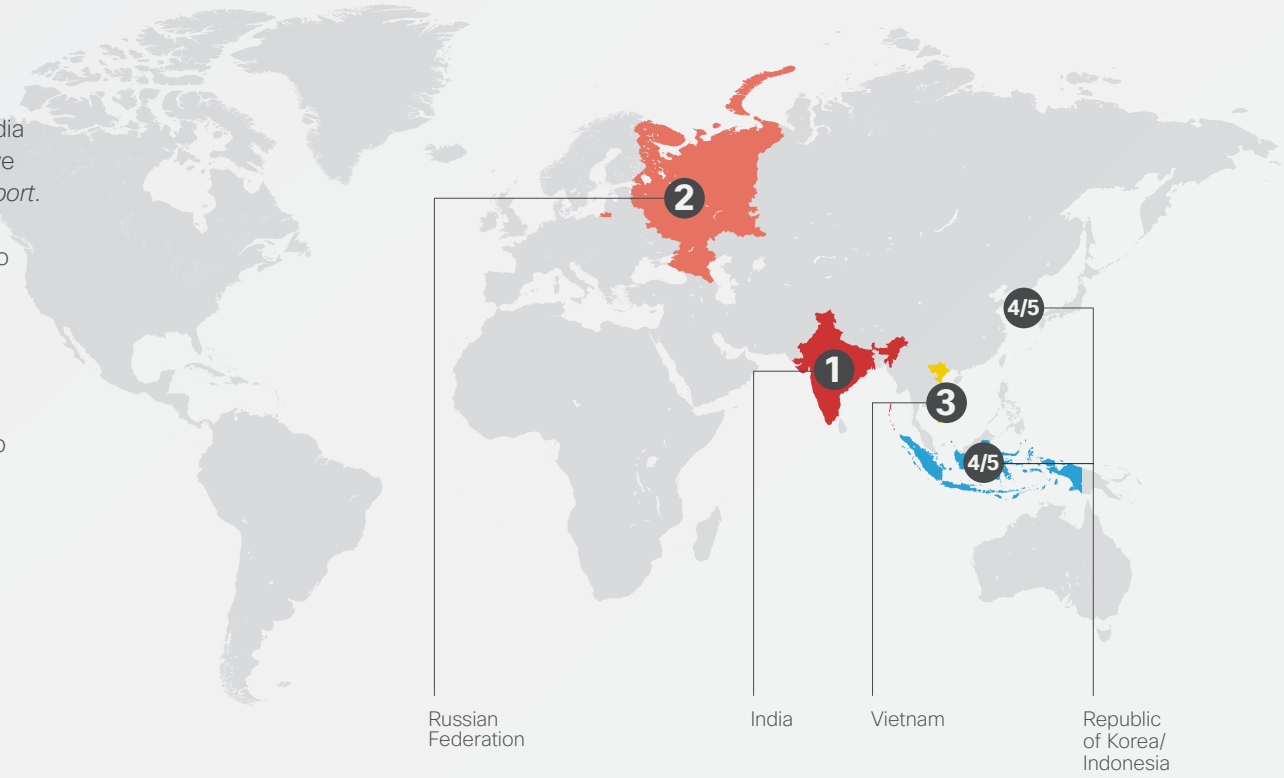
Holding second place on this year's list of spam nations is the Russian Federation, with 7.8 percent. Its spam volume increased during the first half of 2011, rising from 7.6 percent in January to a peak of 9 percent in May, but has been experiencing a steady decline in volume since.

Third on the list for 2011 is Vietnam, which, like India and the Russian Federation, was among the top five spam nations in the *Cisco 2010 Annual Security Report*. Vietnam's spam volume hovered between 3 and 4 percent for much of the year, but then jumped to nearly 6 percent in August 2011 and grew again to nearly 8 percent in September 2011.

Rounding out this year's top five spam nations are the Republic of Korea and Indonesia, each with 6 percent in total spam volume, according to Cisco SIO's research. Neither country appeared among the top 12 spam nations in last year's report.

China, which was seventh on the list in 2010, maintains the same position in the current lineup. However, while that country's spam volume has increased only slightly overall, from 3.6 percent in December 2010 to 4.7 percent in September 2011, it was by far the highest-ranking spam nation for a short period this year. From May to June, China's total spam volume leapt from 1.1 percent to just over 10 percent. Its spam volume peaked at 18 percent in July, and then edged down to 11.5 percent in August before dropping dramatically to 4.7 percent percent in September.

Cisco SIO's research also reveals that Brazil had spam volume of about 4.5 percent in September 2011. Brazil now ranks eighth among the top spam nations, after topping the list in 2009 and earning third place on last year's list. However, the country's spam volumes did fluctuate throughout 2011, nearly doubling to 8 percent by April 2011 before beginning a steady decline to 4.5 percent.



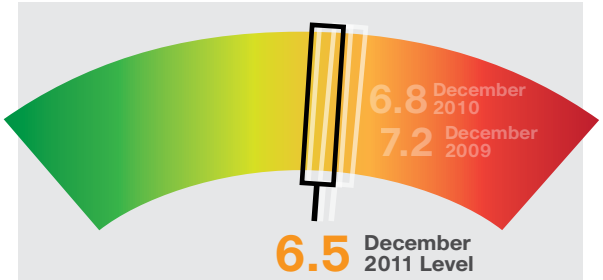
The Cisco Global ARMS Race Index

The annual Cisco Global ARMS Race Index, inspired by the Richter Scale used to measure earthquake magnitude, tracks "Adversary Resource Market Share" (ARMS). The index provides a way to measure the overall level of compromised resources worldwide—the networks and machines currently under "adversarial control." Cisco security experts created the index as a way to gain a better understanding of overall trends based on the global online criminal community's activities and their rates of success at compromising both enterprise and individual users.

According to data collected for this year's index, the aggregate number that represents the level of compromised resources at the end of 2011 is 6.5, down slightly from the December 2010 level of 6.8. When the Cisco Global ARMS Race Index debuted in the *Cisco 2009 Annual Security Report*, the aggregate number was 7.2, which meant enterprise networks at the time were experiencing persistent infections, and consumer systems were infected at levels capable of producing consistent and alarming levels of service abuse.

Since then, consumer and enterprise systems have seen a constant decline in infection rate, but levels are still between "capable of producing consistent and alarming levels of service abuse" and "capable of broad (but not sustained) high-level service abuse." Unfortunately, the magnitude decline does not tell the whole story, as each copy of a criminal's APT malware is doing far more damage than in years past.

What's behind this year's decline in the level of compromised resources worldwide? The decrease in the number of massive botnets driven by law enforcement and botnet takedowns has had a significant impact. As discussed earlier in this report, sophisticated criminal operations are moving away from the massive botnets commonplace in years past because law enforcement and the security industry are keeping a close watch on this activity. However, many smaller botnets have been developed—with each one capable of inflicting more damage per bot.



9.5+: More resources are under rogue control than legitimate control. Inability to trust any connection or application. All services are readily deniable.

9-9.5: Nearly every network, every machine type, every user type, in all regions is infected at significant levels. Widespread resource abuse is common.

8: Enterprise networks are widely and continuously infected. Consumer systems are heavily infected, with traditional security programs proving ineffective. Large simultaneous attacks on many high-visibility targets are possible.

7: Enterprise networks are experiencing persistent infections. Consumer systems are infected at levels capable of producing consistent and alarming levels of service abuse.

6: Enterprise networks are infrequently infected. Consumer systems have significant infection levels and are capable of broad (but not sustained) high-level service abuse.

5: Enterprise networks are rarely infected. Consumer systems are experiencing annoying but not alarming infections; targeted service abuse is possible.

1-4: Enterprise networks are virtually not infected. Consumers have nominal levels of infection and barely noticeable abuse.

According to the Cisco Global ARMS Race Index, the level of resources under adversarial control worldwide was 6.5 at the end of 2011. This is a decline from the 2010 level of 6.8, showing that infections of enterprise networks and consumer systems are less frequent compared to 12 months ago.

Additionally, many in the shadow economy now center their efforts on infecting specific high-value targets with APTs and launching targeted attacks that are more likely to yield a lucrative payout. The prevalence of feature-rich data theft malware such as Zeus/SpyEye has enabled many criminal gangs to launch such attacks. "The 'Ocean's 11' gangs are out there," says Patrick Peterson, senior security researcher for Cisco. "They're focusing tremendous energy on compromising a small number of high-value targets versus the carpet-bombing techniques of the past."

Methodology

To arrive at this year's measurement on the 10-point Cisco Global ARMS Race Index, Cisco relied on leading botnet-tracking estimates of total bots and other data points derived through internal research and other expert sources, such as The Shadowserver Foundation, which tracks cybercriminal activity and is composed of volunteer security professionals from around the world. The methodology for the Global ARMS Race Index is based on:

- **Current aggregate botnet size**
- **Statistics used to estimate the total number of Internet-connected systems in the world**
- **Estimates of home and work infection rates, which measure factors such as resource availability**

The Internet: A Fundamental Human Necessity?

2011 saw the Internet being used in new and powerful ways—in particular, to bring together people on a mass scale to create change that has altered the landscape of our global community. Its influence on our everyday life, both work and personal, is only growing as well. So it begs the question: If we have become so reliant on the Internet and its power to connect us with information and people from anywhere in the world, is it now a fundamental human necessity?

According to one in three college students and young professionals surveyed for *Cisco's Connected World* study, it is. In fact, they consider it to be as important to their lives as air, water, food, and shelter. To some, this attitude may seem extreme, but more than likely, it is a view that will be commonplace among those in the next-generation workforce. While today we observe how the line between personal and professional use of the Internet and Web 2.0 tools and technologies is blurring, soon there may be no discernible delineation whatsoever.

Meanwhile, there is no question that for today's businesses, the Internet is a necessity—for both basic operations and competitive advantage. For that reason alone, it would seem there should be no debate in the enterprise around whether any technology that will significantly enhance productivity, efficiency, and innovation—and the satisfaction of workers—should be embraced and put in use strategically throughout the organization. However, many businesses are finding it difficult to adapt to so much change so quickly. They cite security concerns as a primary hurdle to leveraging new technologies. But many are beginning to understand that a wait-and-see approach, while meant to protect the enterprise and its assets, may actually undermine their competitive edge—if not now, then definitely in the future.

Moving too slowly doesn't just mean that enterprises risk taking advantage of innovations that can help their business achieve new levels of success. They also risk not being able to recruit or retain their most important asset: talent. As discussed in this report, many of today's employees would be inclined not to take a job if a potential employer told them their access to corporate networks and applications would be severely limited or prohibited. (See "Remote Access and BYOD: Enterprises Working to Find Common Ground with Employees," page 10.)

Likewise, more than half of college students surveyed for the *Connected World* study said if they encountered a company that banned access to social media, they would either not accept a job with that organization, or would join and find a way to access social media despite corporate policies. (See "Social Media: Now It's a Productivity Tool," page 8.)

But many enterprises are trying to change. Cisco security experts interviewed for the *2011 Annual Security Report* have reported seeing many firms making strides in both evolving their security model so it is relevant for today's connected world, and in trying to find common ground with employees who are demanding access to applications and devices that they want to use for work. They're also re-evaluating their AUPs and business codes of conduct, reinvigorating their DLP efforts, and taking the enterprise security discussion—and the responsibility for preserving desired levels of security—beyond the IT function and into departments throughout the organization, from marketing to human resources and legal right up to the management level.

As we've learned in this report, Cisco is among them. Like countless organizations worldwide, it is working to find the right balance between seizing new opportunities and maintaining network and data security. Cisco's "Any Device" initiative, designed to allow the company's employees greater choice in devices, while maintaining a common, predictable user experience that maintains or enhances global organizational competitiveness and

> "The rapid erosion of this perimeter that took 20 years to build has left many enterprises stunned and feeling vulnerable as they embark on the BYOD journey."
>
> —Ofer Elzam, integrated security solutions architect, Cisco

security, is an important start. However, even building the foundation for movement toward a BYOD model can be a challenge.

"Modern smartphones and tablets are a huge IT disruption," says Ofer Elzam, integrated security solutions architect for Cisco. "Enterprises are conditioned to maintaining a defined security perimeter and fiercely protecting everything inside of it. The rapid erosion of this perimeter that took 20 years to build has left many enterprises stunned and feeling vulnerable as they embark on the BYOD journey."

In many ways, their feelings of vulnerability are not misplaced. While living in a connected world means we are closer to our co-workers, business partners, customers, friends, and family, we and the organizations we work for and do business with are also within easier reach of the criminal economy. The openness and interconnectedness that mobile devices, social networks, and Web 2.0 applications support provide new avenues for malicious actors to steal from others, disrupt business, or simply, make a statement.

Cybercriminals are investing more toward "R&D" to find ways to use mobile devices and penetrate the cloud to seize the data they need to make a profit or undermine a company's success. And as the hacktivism trend clearly indicates, today's technology allows like-minded social disrupters and criminals to connect and assemble quickly, anonymously, and unpredictably for a specific goal that may not be motivated by money or have a purpose that is easy for others, including targets, to decipher. "Some of the things we've witnessed over the past year are like nothing we've ever seen before," says Gavin Reid, Cisco CSIRT manager. "Some events have been absolutely crushing, and this is not a good sign."

Like our own planet, the connected world has a light side and dark side at all times. Enterprise security can exist here, but building an effective model requires new thinking as well as some risk-taking—and maintaining it demands more vigilance than ever before. The core challenge for today's businesses is that they must find the right mix of technology and policy to meet their unique combination of needs. This is not an easy process, but the end result will be a more agile business better prepared to adapt—both swiftly and securely—to changes in technology that tomorrow inevitably will bring.

"The connected world is a more fluid world. And it's literally 'sink or swim' time now for enterprises that have yet to accept that change is no longer just at their door—it's already in their workplace," says Chris Young, senior vice president for the Security Group at Cisco. "By embracing the technologies that their employees, and their customers, inevitably will use, enterprises can create a better overall security solution by addressing reality instead of wondering about the 'what if.'"

2012 Action Items for Enterprise Security

Even though organizations need to develop an approach to network and data security that will support the specific needs of their workforce and help them to achieve key business objectives, there are several things that any enterprise can do to improve its security posture both immediately and over the long term. Following are 10 recommendations from Cisco's security experts:

1 Assess the totality of your network. "Know where your IT infrastructure begins and ends—so many enterprises simply have no idea of the entirety of their network. Also, know what your 'normal' is so you can quickly identify and respond to a problem."

John N. Stewart, vice president and chief security officer for Cisco

2 Re-evaluate your acceptable use policy and business code of conduct. "Get away from the laundry list approach with security policies. Focus only on those things you know you must and can enforce."

Gavin Reid, Cisco CSIRT manager

3 Determine what data must be protected. "You cannot build an effective DLP program if you don't know what information in the enterprise must be secured. You also must determine who in the enterprise is allowed to have access to that information, and how they are allowed to access it."

David Paschich, web security product manager for Cisco

4 Know where your data is and understand how (and if) it is being secured. "Identify every third party that has permission to store your company's data—from cloud providers to email marketers—and confirm that your information is being secured appropriately. Compliance requirements, and now the trend in cybercrime toward 'hack one to hack them all,' means enterprises must never assume their data is secure, even when they put it in the hands of those they trust."

Scott Olechowski, threat research manager for Cisco

5 Assess user education practices. "Long seminars and handbooks aren't effective. Younger employees will be more receptive to a targeted approach to user education, with shorter sessions and 'just-in-time' training. Peer training also works well in today's collaborative work environment."

David Evans, chief futurist for Cisco

6 Use egress monitoring. "This is a basic thing, but not enough enterprises do it—although compliance demands have more organizations adopting this practice. Egress monitoring is a change in focus from just blocking 'the bad' from coming in. You monitor what is being sent out of your organization and by whom and to where—and block things from leaving that shouldn't be."

Jeff Shipley, manager for Cisco Security Research and Operations

7 Prepare for the inevitability of BYOD. "Organizations need to stop thinking about *when* they are going to move to a BYOD model and start thinking more about *how*."

Nasrin Rezai, senior director of security architecture and chief security officer for Cisco's Collaboration Business Group

8 Create an incident response plan. "IT-related risk should be treated like any other business risk. This means enterprises need to have a clear plan in place to respond quickly and appropriately to any type of security event, whether it's a data breach resulting from a targeted attack, a compliance violation due to an employee's carelessness, or an incident of hacktivism."

Pat Calhoun, vice president and general manager of Cisco's Secure Network Services Business Unit

9 Implement security measures to help compensate for lack of control over social networks. "Do not underestimate the power of technology controls, such as an intrusion prevention system for protecting against network threats. Reputation filtering is also an essential tool for detecting suspicious activity and content."

Rajneesh Chopra, director of product management, Cisco Security Technology Group

10 Monitor the dynamic risk landscape and keep users informed. "Enterprises and their security teams need to be vigilant about a much broader range of risk sources, from mobile devices and the cloud to social networking and whatever new technology tomorrow may bring. They should take a two-step approach: reacting to security vulnerability disclosures, while also being proactive about educating their employees on how to protect themselves and the enterprise from persistent and potent cyber threats."

Ofer Elzam, integrated security solutions architect for Cisco

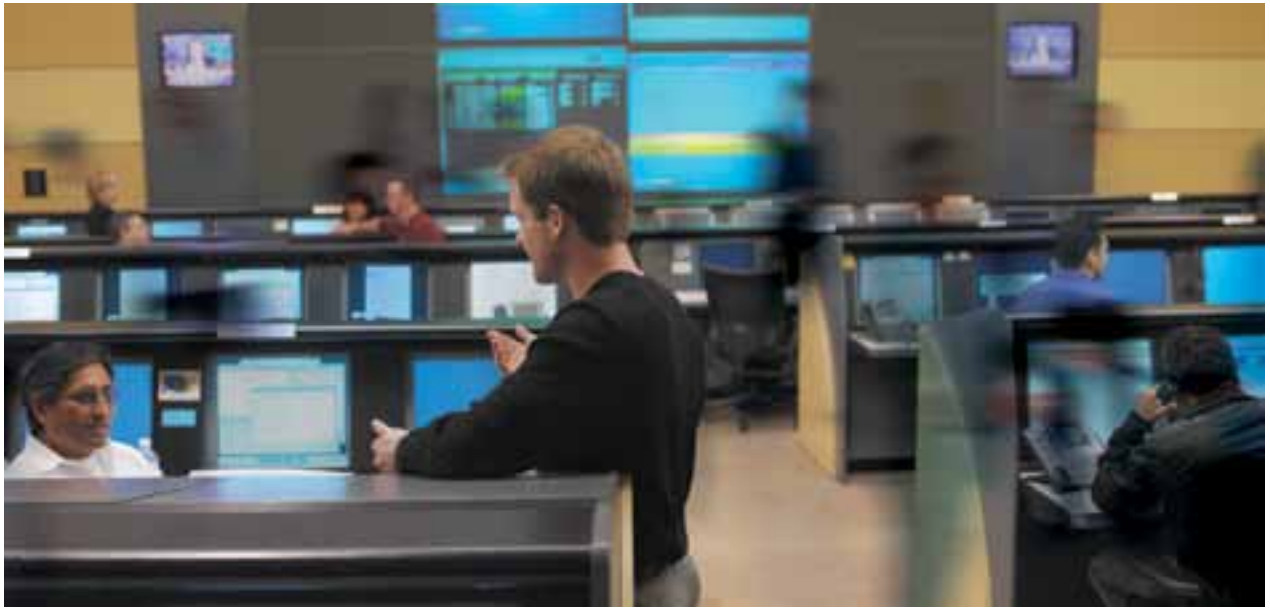
Cisco Security Intelligence Operations

It has become an increasing challenge to manage and secure today's distributed and agile networks. 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 stays ahead of the latest threats using real-time threat intelligence from Cisco Security Intelligence Operations (SIO). Cisco SIO is the world's largest cloud-based security ecosystem, using SensorBase data of almost 1 million live data feeds from deployed Cisco email, web, firewall, and intrusion prevention system (IPS) solutions.

Cisco SIO weighs and processes the data, automatically categorizing threats and creating rules using more than 200 parameters. Security researchers also collect and supply information about security events that have the potential for widespread impact on networks, applications, and devices. Rules are dynamically delivered to deployed Cisco security devices every three to five minutes. The Cisco SIO team also publishes security best practice recommendations and tactical guidance for thwarting threats.

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



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/trialdo?dispatch=4

For early-warning intelligence, threat and vulnerability analysis, and proven Cisco mitigation solutions, please visit: www.cisco.com/go/sio.

Cisco SecureX

The Cisco SecureX architecture is a next-generation, context-aware framework that meets the evolving security needs of borderless network environments.

Unlike legacy security architectures that were built to enforce policies based on a single data point, Cisco SecureX enforces policies based on the full context of the situation. Context-aware policies use a high-level language that aligns closely to business policy. This greatly simplifies policy administration while simultaneously providing more effective security and control. As a result, networks are far more secure, while business efficiency and flexibility are maximized.

The Cisco SecureX architecture:

Enforces context-aware policy across a wide range of form factors to deliver security flexibly, when and where you need it.

Manages context-aware security policies throughout the network, providing deep insights into–and effective controls over–who is doing what, when, where, and how.

Provides secure access from a full range of devices–from traditional PCs and Mac-based computers, to smartphones, tablets, and other mobile devices–anytime, anywhere.

Leverages Cisco SIO for robust, real-time insights into the global threat environment.

Enables simplified business policies that will correlate directly between what IT must enforce and the organization's business rules.

Integrates comprehensive, extensible APIs that allow Cisco's own management systems and partners to plug in and complete the security ecosystem.

For more information on Cisco SecureX, go to www.cisco.com/en/US/netsol/ns1167/index.html.

For More Information

Cisco Security Intelligence Operations
www.cisco.com/security

Cisco Security Blog
blogs.cisco.com/security

Cisco Remote Management Services
www.cisco.com/en/US/products/ps6192/serv_category_home

Cisco Security Products
www.cisco.com/go/security

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.