2015

Annual Security Report

Executive Summary

As dynamic as the modern threat landscape is, there are some constants.

Adversaries are committed to continually refining or developing new techniques that can evade detection and hide malicious activity. Meanwhile, the defenders—namely, security teams—must constantly improve their approach to protecting the organization and users from these increasingly sophisticated campaigns.

Caught in the middle are the users. But now, it appears they not only are the targets, but also the complicit enablers of attacks.

The *Cisco 2015 Annual Security Report*, which presents the research, insights, and perspectives provided by Cisco® Security Research and other security experts within Cisco, explores the ongoing race between attackers and defenders, and how users are becoming ever-weaker links in the security chain.

Cybersecurity is a broad and complex topic that has a far-reaching impact on users, companies, governments, and other entities around the world. The *Cisco 2015 Annual Security Report* is divided into four areas of discussion. These sections, and the issues explored within them, may at first glance seem disparate, but closer examination reveals their interconnectedness:

Four discussion areas of the *Cisco 2015 Annual Security Report:*

1. Threat Intelligence
2. Cisco Security Capabilities Benchmark Study
3. Geopolitical and Industry Trends
4. Changing the View Toward Cybersecurity—From Users to the Corporate Boardroom

1. Threat Intelligence

This section provides an overview of the latest threat research from Cisco, including updates on exploit kits, spam, threats and vulnerabilities, and malvertising (malicious advertising) trends. Online criminals' growing reliance on users to help launch their attacks is also examined. To produce their analysis of observed trends in 2014, Cisco Security Research utilized a global set of telemetry data. The threat intelligence provided in the report represents work conducted by top security experts across Cisco.

2. Security Capabilities Benchmark Study

To gauge perceptions of security professionals on the state of security in their organizations, Cisco asked chief information security officers (CISOs) and security operations (SecOps) managers in nine countries and at organizations of different sizes about their security resources and procedures. The study's findings are exclusive to the *Cisco 2015 Annual Security Report.*

3. Geopolitical and Industry Trends

In this section, Cisco security, geopolitical, and policy experts identify current and emerging geopolitical trends that organizations—particularly, multinational companies—should monitor. In focus: how cybercrime is flourishing in areas of weak governance. Also covered are recent developments around the world related to the issues of data sovereignty, data localization, encryption, and data compatibility.

4. Changing the View Toward Cybersecurity—From Users to the Corporate Boardroom

Cisco security experts suggest that it is time for organizations to start viewing their approach to cybersecurity differently if they want to achieve real-world security. Strategies include adopting more sophisticated security controls to help defend against threats before, during, and after an attack; making security a topic at the corporate boardroom level; and implementing the Cisco Security Manifesto, a set of security principles that can help organizations become more dynamic in their approach to security—and more adaptive and innovative than adversaries.

The interconnectedness of the security topics covered in the *Cisco 2015 Annual Security Report* comes down to this: Attackers have become more proficient at taking advantage of gaps in security to hide and conceal their malicious activity. Users—and security teams—are both part of the security problem. While many defenders believe their security processes are optimized—and their security tools are effective—in truth, their security readiness likely needs improvement. What happens in the geopolitical landscape, from legislation to security threats, can have a direct impact on business operations and how an organization addresses security. And taking into consideration all these factors, it has never been more critical for organizations of all sizes to understand that security is a people problem, that compromise is inevitable, and that the time to take a new approach to security is now.

Key Discoveries

Following are key discoveries presented in the Cisco 2015 Annual Security Report.

Attackers have become more proficient at taking advantage of gaps in security to hide and conceal malicious activity.

- In 2014, 1 percent of high-urgency common vulnerabilities and exposure (CVE) alerts were actively exploited. This means organizations must prioritize and patch that 1 percent of all vulnerabilities quickly. But even with leading security technology, excellence in process is required to address vulnerabilities.
- Since the Blackhole exploit kit was sidelined in 2013, no other exploit kit has been able to achieve similar heights of success. However, the top spot may not be as coveted by exploit kit authors as it once was.
- Java exploits have decreased by 34 percent, as Java security improves and adversaries move to embrace new attack vectors.
- Flash malware can now interact with JavaScript to help conceal malicious activity, making it much harder to detect and analyze.
- Spam volume increased 250 percent from January 2014 to November 2014.
- Snowshoe spam, which involves sending low volumes of spam from a large set of IP addresses to avoid detection, is an emerging threat.

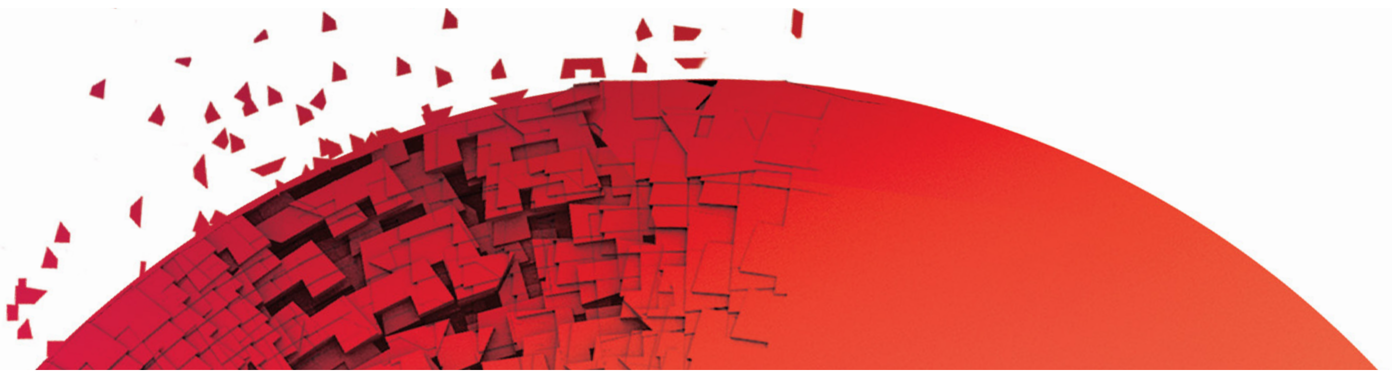
Users and IT teams have become unwitting parts of the security problem.

- Online criminals rely on users to install malware or help exploit security gaps.
- Heartbleed, the dangerous security flaw, critically exposes OpenSSL. Yet 56 percent of all OpenSSL versions are older than 50 months and are therefore still vulnerable.
- Users' careless behavior when using the Internet, combined with targeted campaigns by adversaries, places many industry verticals at higher risk of web malware exposure. In 2014, the pharmaceutical and chemical industry emerged as the number-one highest-risk vertical for web malware exposure, according to Cisco Security Research.
- Malware creators are using web browser add-ons as a medium for distributing malware and unwanted applications. This approach to malware distribution is proving successful for malicious actors because many users inherently trust add-ons or simply view them as benign.

The *Cisco Security Capabilities Benchmark Study* reveals disconnects in perceptions of security readiness.

- Fifty-nine percent of chief information security officers (CISOs) view their security processes as optimized, compared to 46 percent of security operations (SecOps) managers.
- About 75 percent of CISOs see their security tools as very or extremely effective, with about one-quarter perceiving security tools as only somewhat effective.
- Ninety-one percent of respondents from companies with sophisticated security strongly agree that company executives consider security a high priority.
- Less than 50 percent of respondents use standard tools such as patching and configuration to help prevent security breaches.
- Larger, midsize organizations are more likely to have highly sophisticated security postures, compared to organizations of other sizes included in the study.

Table of Contents



Attackers vs. Defenders: An Ongoing Race

Security professionals and online criminals are in an ongoing race to see which side can outwit the other.

On the security side, organizations appear to have upped their game by adopting more sophisticated tools for preventing attacks and reducing their impact. They've recognized the business necessity of a strong security posture—and express confidence that their security processes are optimized. Technology vendors are also more attentive toward finding and fixing vulnerabilities in their products, giving criminals fewer opportunities to launch exploits.

But at the same time, adversaries are becoming more sophisticated not only in their approaches to launching attacks, but also in evading detection:

- They change their tactics and tools from moment to moment, disappearing from a network before they can be stopped, or quickly choosing a different method to gain entry.
- They devise spam campaigns using hundreds of IP addresses in an attempt to bypass IP-based anti-spam reputation products.
- They design malware that relies on tools that users trust, or view as benign, to persistently infect and hide in plain sight on their machines.
- They find new vulnerabilities to exploit if vendors shut down weaknesses in other products.
- They work at establishing a hidden presence or blend in with the targeted organization, sometimes taking weeks or months to establish multiple footholds in infrastructure and user databases. Only when they are ready will they execute their core mission.

According to the new *Cisco Security Capabilities Benchmark Study* (see page 24), security professionals say they're optimistic that they're well prepared to hold back online attackers. Yet adversaries continue to steal information, make money through scams, or disrupt networks for political goals. In the end, security is a numbers game: Even if an organization blocks 99.99 percent of billions of spam messages, some will make it through. There is no way to ensure 100 percent effectiveness.

When these messages or exploits manage to reach users, it is the users themselves who become the weak point in the network. Since enterprises have become more adept at using solutions that block network breaches, malware, and spam, malicious actors may instead exploit users through tactics such as sending them a fake request for a password reset.

With users becoming ever-weaker links in the security chain, enterprises have choices to make when implementing security technologies and policies: As developers try to make applications and software more intuitive and easy to use, do organizations open new loopholes for cybercriminals to exploit? Do enterprises bypass users, assuming they cannot be trusted or taught, and install stricter security controls that impede how users do their jobs? Do they take the time to educate users on why security controls are in place, and clearly explain how users play a vital role in helping the organization achieve dynamic security that supports the business?

As the principles outlined in the Cisco Security Manifesto on page 45 suggest, it is the latter. Technology solutions rarely empower users to take charge of security as active participants. Instead, they force them to work around security tools that get in the way of their workday—thus leaving the business less secure. Security is no longer a question of *if* a network will be compromised. Every network *will,* at some point, be compromised. What will an organization do then? And if security staff knew the network was going to be compromised, would it approach security differently?

The *Cisco 2015 Annual Security Report* presents the latest research from its Cisco Security Research group. The team examines security industry advances designed to help organizations and users defend against attacks, and the techniques and strategies employed by adversaries hoping to break through those defenses. The report also highlights key findings from the *Cisco Security Capabilities Benchmark Study,* which examines the security posture of enterprises and their perceptions of their preparedness to defend against attacks. Geopolitical trends, global developments around data localization, the value of more sophisticated secure access controls, segmentation based on role-based access, and the importance of making cybersecurity a boardroom topic are also discussed.

1. Threat Intelligence

Cisco Security Research has assembled and analyzed security insights in this report based on a global set of telemetry data. Cisco security experts perform ongoing research and analysis of discovered threats, such as malware traffic, which can provide insights on possible future criminal behavior and aid in the detection of threats.

Web Exploits: For Exploit Kit Authors, Holding the Top Spot May Not Mean You're the Best

In the business world, companies strive to be known as industry leaders. But for exploit kit authors operating in the so-called "shadow economy," maintaining fourth or fifth position among leading exploit kits may be an even more telling sign of success, according to Cisco Security Research.

As reported in the *Cisco 2014 Midyear Security Report,* there has been no clear leader among exploit kits since late 2013.[1] That's when authorities sidelined the widely used, well-maintained, and highly effective Blackhole exploit kit after arresting its alleged creator and distributor, known as "Paunch." Cisco Security Research suggests that a key reason no dominant exploit kit exists—yet—is simply because no other kit has emerged as a true technological leader among contenders. Another trend observed: Since takedown of Paunch and Blackhole, more exploit kit users appear to be taking care to invest in kits known to be technically sophisticated in terms of their ability to evade detection.

Throughout 2014, Angler, Sweet Orange, and Goon were the exploit kits observed most often "in the wild," according to Cisco security experts. Among all exploit kits, Angler was detected in the field most frequently during 2014, and for reasons that are unclear, was especially prevalent in late August. Cisco Security Research attributes Angler's popularity to the decision by its author(s) to eliminate the requirement of downloading a Windows executable to deliver malware.

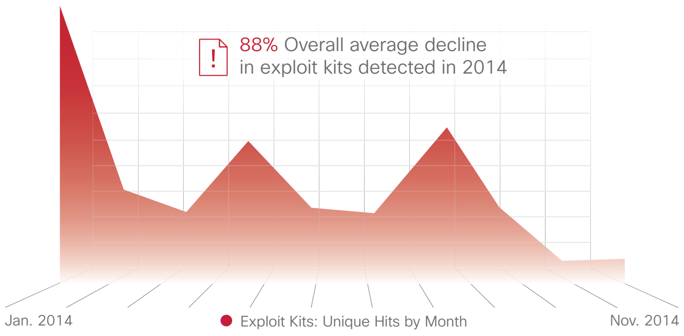
Angler's use of Flash, Java, Microsoft Internet Explorer (IE), and even Silverlight vulnerabilities makes this exploit kit the "one to watch," say Cisco researchers. Once the exploit is triggered, the malware payload is written directly into memory in a process such as iexplore.exe, instead of being written to a disk. The payload delivered by Angler looks like a blob of encrypted data, which makes it harder to identify and block.

To learn more about Angler, and how malvertising (malicious advertising) is used as a primary avenue for delivering the exploit kit to users, see the Cisco Security blog post, "Angling for Silverlight Exploits."

The Sweet Orange exploit kit is also very dynamic; its components, ports, and payload URLs change constantly so that Sweet Orange can remain effective and avoid detection. This positions Sweet Orange as the "most likely to succeed" among exploit kits, according to Cisco Security Research. Sweet Orange distributes a range of malware to unpatched end-user systems, and includes exploits for vulnerabilities in Adobe Flash Player, IE, and Java. Adversaries who use Sweet Orange often rely on malvertising to redirect users to websites—including legitimate sites—that host the exploit kit. Users are usually redirected at least twice in the process. Compromised websites running outdated versions of content management systems (CMS) such as WordPress and Joomla are other locations known to be ripe for hosting the Sweet Orange exploit kit.[2]

As for the Goon exploit kit, Cisco Security Research points to its reputation for reliability as the likely reason for its modest but consistent popularity in 2014; it also has earned the distinction of being "the most organized" compared to other exploit kits. Originally discovered by security researchers in 2013, Goon—known also as the "Goon/Infinity exploit kit"—is a malware distribution framework that generates exploits for browser vulnerabilities pertaining to Flash, Java, or Silverlight components on Windows and Mac platforms.[3]

Figure 1. Exploit Kit Trends: Number of Unique Hits Detected from January to November 2014



Source: Cisco Security Research

Read the Cisco Security blog post, "Fiesta Exploit Pack Is No Party for Drive-By Victims," to find out how companies can defend against the Fiesta exploit kit. This kit delivers malware through attack vectors such as Silverlight and uses dynamic DNS domains (DDNS) as exploit landing pages.

For details on the Nuclear exploit kit, and its ability to assess a user's system to determine vulnerabilities and deliver appropriate malware types, see the Cisco Security blog post, "Evolution of the Nuclear Exploit Kit."

While the overall number of exploit kits detected in the field had dropped by 87 percent in the months following the demise of the Blackhole exploit kit, the number of kits detected by Cisco Security Research increased over the summer of 2014 (see Figure 1). In the last two weeks of August, they observed a significant spike in the number of detections in the field of the Angler exploit kit. However, by November, the overall number of detections of known exploit kits had once again declined, with Angler and Goon/Infinity still showing up most frequently. The overall average decline in the number of exploit kits detected between May and November 2014 is 88 percent.

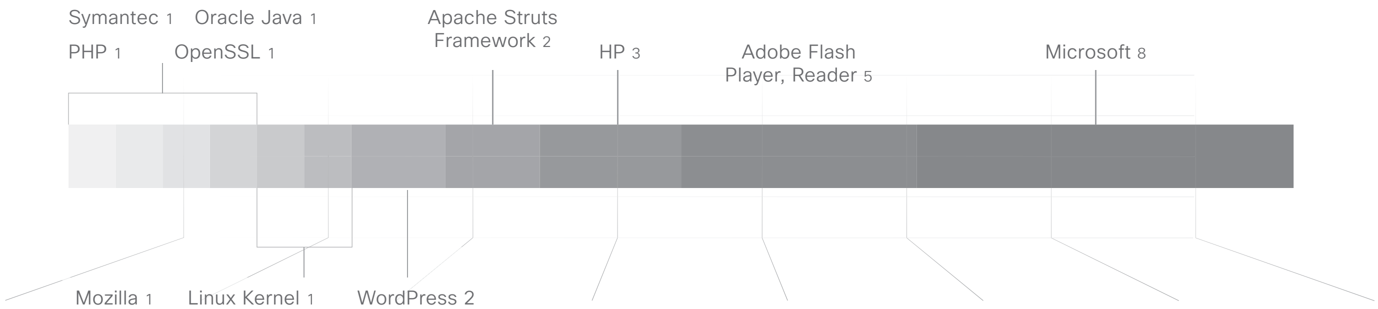
Threats and Vulnerabilities: Java Declines as an Attack Vector

In recent years, Java has played an unwanted starring role in lists of the most prevalent and severe vulnerabilities to exploit. However, Java appears to be falling out of favor among adversaries searching for the fastest, easiest, and least detectable ways to launch exploits using software vulnerabilities, according to Cisco Security Research.

Of the top 25 vendor- and product-related vulnerability alerts from January 1, 2014, to November 30, 2014, only one was Java-related (see Table 1's Common Vulnerability Scoring System [CVSS] chart on page 10). In 2013, Cisco Security Research tracked 54 urgent new Java vulnerabilities; in 2014, the number of tracked Java vulnerabilities fell to just 19. This should not detract online criminals from the popularity and effectiveness of attacking these older vulnerabilities that persist today.

Data from the National Vulnerability Database (NVD) shows a similar decline: NVD reported 309 Java vulnerabilities in 2013 and 253 new Java vulnerabilities in 2014. (Cisco Security Research tracks significant vulnerabilities that score high on the CVSS scale, hence the lower number, while the NVD includes all reported vulnerabilities.) Figure 2 outlines top vulnerability exploits by vendor and product in 2014.

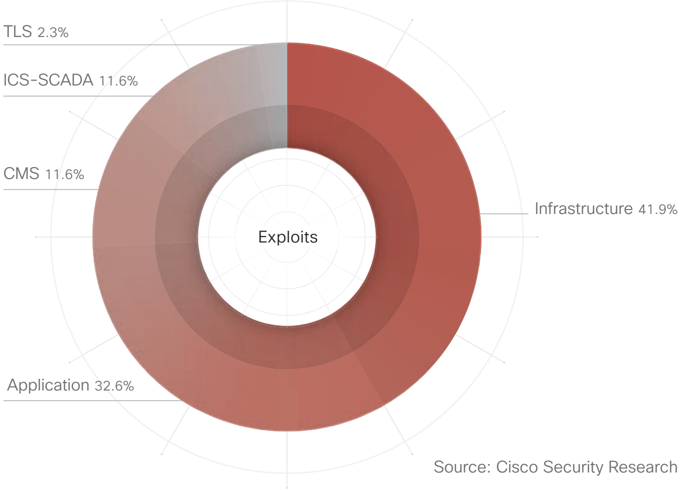
Figure 2. Top Vendor and Product Vulnerability Exploits



Source: Cisco Security Research

Share the report

Figure 3. Top Product Categories Exploited



Source: Cisco Security Research

Exploits involving client-side vulnerabilities in Adobe Flash Player and Microsoft IE have taken the lead away from Java, along with exploits that target servers (for example, exploits involving vulnerabilities in Apache Struts Framework, the open-source web framework). The growing number of Apache Struts Framework exploits is an example of the trend toward criminals compromising online infrastructure as a way to expand their reach and ability during their attacks.

The Apache Struts Framework is a logical starting point for exploits due to its popularity.

Figure 3 highlights the most popular product categories that were exploited in 2014.

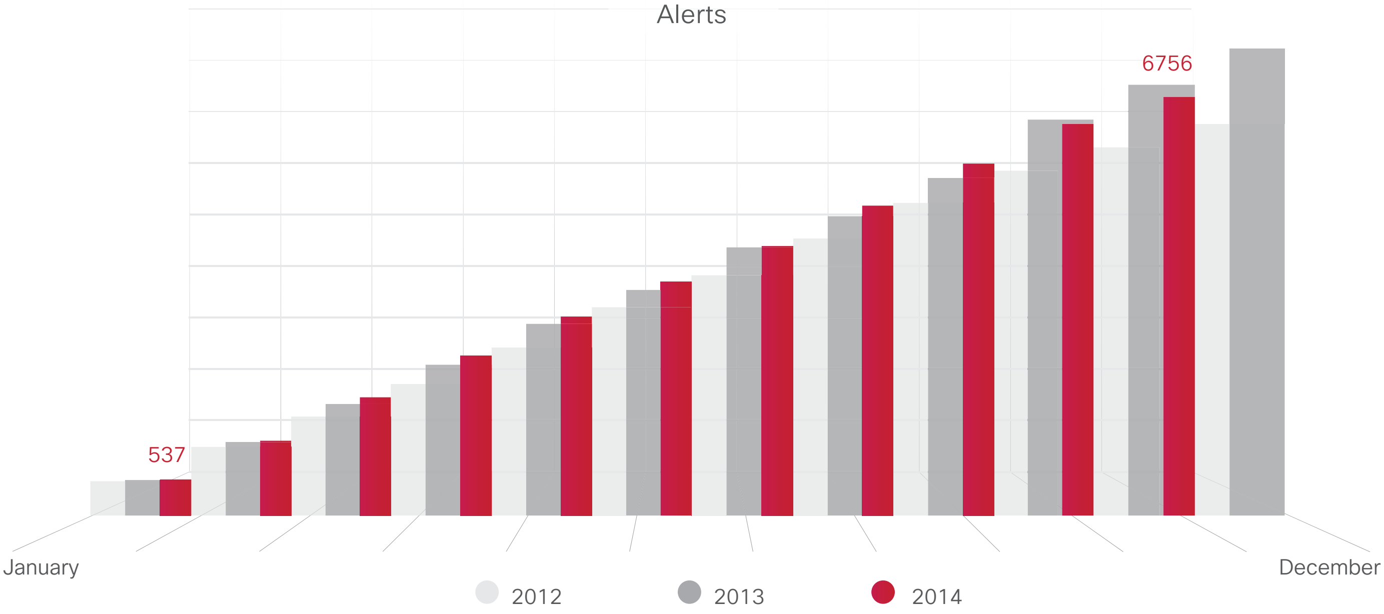
In 2014, applications and infrastructure were the most frequently exploited, according to Cisco Security Research data. Content management systems (CMS) are also preferred targets; adversaries rely on websites running outdated versions of CMS to facilitate exploit delivery

Cumulative Annual Alerts on a Decline

Annual alert totals, the cumulative new and updated product vulnerabilities reported in 2014 and compiled by Cisco Security Research, appear to be on the decline (Figure 4). As of November 2014, total alerts fell below 2013 totals by 1.8 percent. The percentage may be small, but it is the first time in recent years that alerts have fallen in number compared to the previous year.

The most likely reason for the decline is the growing attention to software testing and development on the part of vendors. Improved development lifecycles appear to reduce the number of vulnerabilities that criminals can easily exploit.

Figure 4. Cumulative Annual Alert Totals



Source: Cisco Security Research

Share the report

Table 1. Most Commonly Exploited Vulnerabilities

Common Vulnerability Scoring System (CVSS)

IntelliShield ID	Headline	Urgency	Credibility	Severity	Base	Temporal
33695	OpenSSL TLS/DTLS Heartbeat Information Disclosure Vulnerability	■■■■■	■■■■■	■■■□□	5.0	5.0
35880	GNU Bash Environment Variable Content Processing Arbitrary Code Execution Vulnerability	■■■■■	■■■■■	■■■■□	10.0	7.4
35879	GNU Bash Environment Variable Function Definitions Processing Arbitrary Code Execution Vulnerability	■■■■■	■■■■■	■■■■□	10.0	7.4
36121	Drupal Core SQL Injection Vulnerability	■■■■■	■■■■■	■■■■□	7.5	6.2
32718	Adobe Flash Player Remote Code Execution Vulnerability	■■■■■	■■■■■	■■■■□	9.3	7.7
33961	Microsoft Internet Explorer Deleted Memory Object Code Execution Vulnerability	■■■■■	■■■■■	■■■■□	9.3	7.7
28462	Oracle Java SE Security Bypass Arbitrary Code Execution Vulnerabilities	■■■■■	■■■■■	■■■■□	9.3	7.7
30128	Multiple Vendor Products Struts 2 Action: Parameter Processing Command Injection Vulnerability	■■■■■	■■■■■	■■■■■	10.0	8.3

Source: Cisco Security Research

New Alerts vs. Updated Alerts

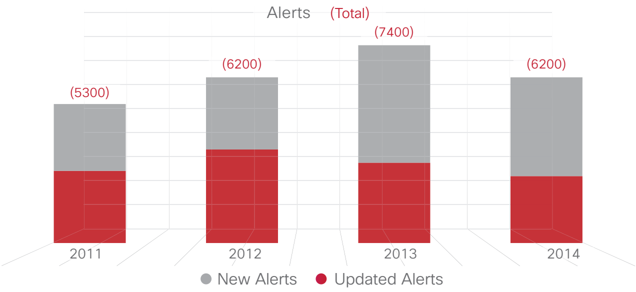
The number of new alerts for 2013 and 2014 indicates that more new vulnerabilities continue to be reported than in previous years, meaning that vendors, developers, and security researchers are finding, fixing, and reporting more new vulnerabilities in their products. As shown in Figure 5, the total number of new alerts and the annual total are even or slightly declining in 2014 compared to 2013.

Table 1 illustrates some of the most commonly exploited vulnerabilities, according to the Common Vulnerability Scoring System (CVSS). The U.S. National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD) provides a framework for communicating the characteristics and impacts of IT vulnerabilities and supports the CVSS. The "Urgency" score in the CVSS table indicates that these vulnerabilities are being actively exploited, which corresponds to the "Temporal" scores indicating active exploits. By scanning the list of products being exploited, enterprises can also determine which of these products are in use and therefore need to be monitored and patched.

Figure 6 depicts the vendors and products with the highest CVSS scores. Cisco indicates through the CVSS score that a proof-of-concept exploit code exists; however, the code is not known to be publicly available.

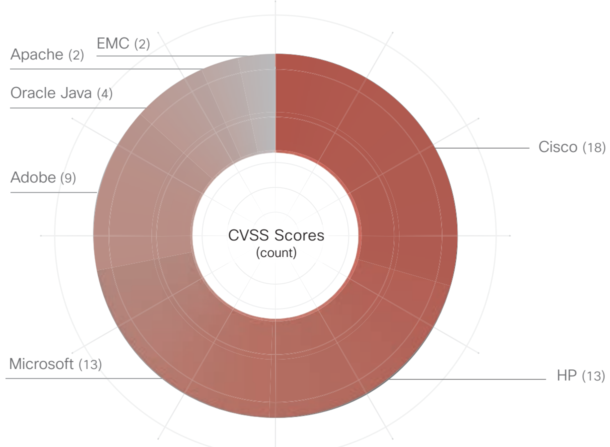
Note: The vulnerabilities in Table 1 were those showing initial signs of exploit activity during the period observed. The majority of these vulnerabilities had not yet gone mainstream, meaning they had not made their way into exploit kits for sale.

Figure 5. Comparison of New Alerts and Updated Alerts



Source: Cisco Security Research

Figure 6. Vendors and Products with the Highest CVSS Scores



Source: Cisco Security Research

Share the report

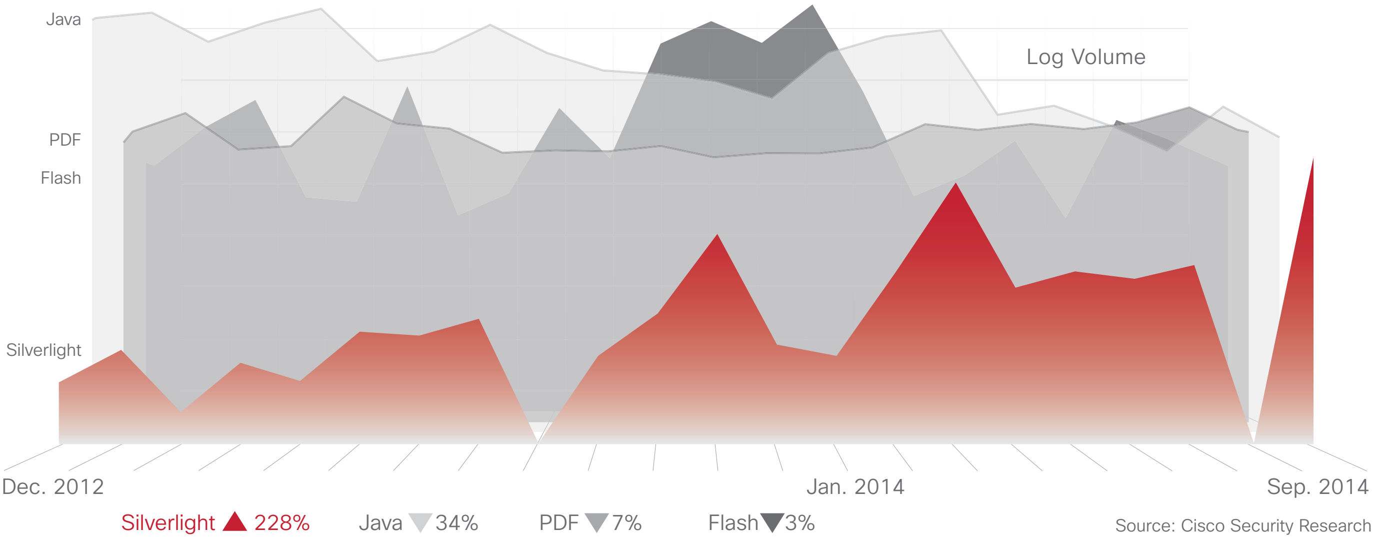
Analysis: Likely Factors for Adversaries Abandoning Java Exploits

Cisco Security Research suggests that the decline in Java exploits can be tied partly to the fact that there were no new zero-day Java exploits disclosed and available for adversaries to take advantage of in 2014. Modern versions of Java automatically patch, and older, more vulnerable versions of the Java Runtime Environment are being blocked by default by browser vendors. Apple is even taking the extra step of disabling old and vulnerable versions of Java and patching them through automatic updates. In addition, the U.S. Computer Emergency Readiness Team (US-CERT) has been recommending since January 2013 that computer users secure, disable, or remove Java.

The latest version of Java, Java 8, has stronger controls than previous releases. It is also harder to exploit because it now requires human interaction, like code signing and a user dialogue that asks the user to enable Java. Online criminals have discovered easier targets and have turned their attention to non-Java vectors that deliver higher return on investment. For example, many users fail to update Adobe Flash and PDF readers or browsers regularly, providing criminals with a wider range of both old and new vulnerabilities to exploit. And as reported in the *Cisco 2014 Midyear Security Report,* the number of exploit kits that include Microsoft Silverlight exploits is growing.[4]

Figure 7 shows that Java's reign as the top attack vector has been on a steady downward trend for more than a year. The use of Flash to launch exploits has been somewhat erratic, with the biggest spike occurring in January 2014. PDF use has been constant, as many malicious actors appear to remain focused on launching highly targeted campaigns through email using PDF attachments. Silverlight attacks, while still very low in number compared to more established vectors, are on the rise—especially since August.

Figure 7. Comparison of Volume Trends by Attack Vector



Source: Cisco Security Research

Flash and JavaScript: Better Together?

In 2014, Cisco Security Research observed growth in the use of Flash malware that interacts with JavaScript. The exploit is shared between two different files—one Flash, one JavaScript. Sharing exploits over two different files and formats makes it more difficult for security devices to identify and block the exploit, and to analyze it with reverse engineering tools. This approach also helps adversaries to be more efficient and effective in their attacks. For example, if the first stage of an attack is entirely in JavaScript, then the second stage, the payload transmission, would not occur until after the JavaScript executes successfully. This way, only users who can run the malicious file receive the payload.

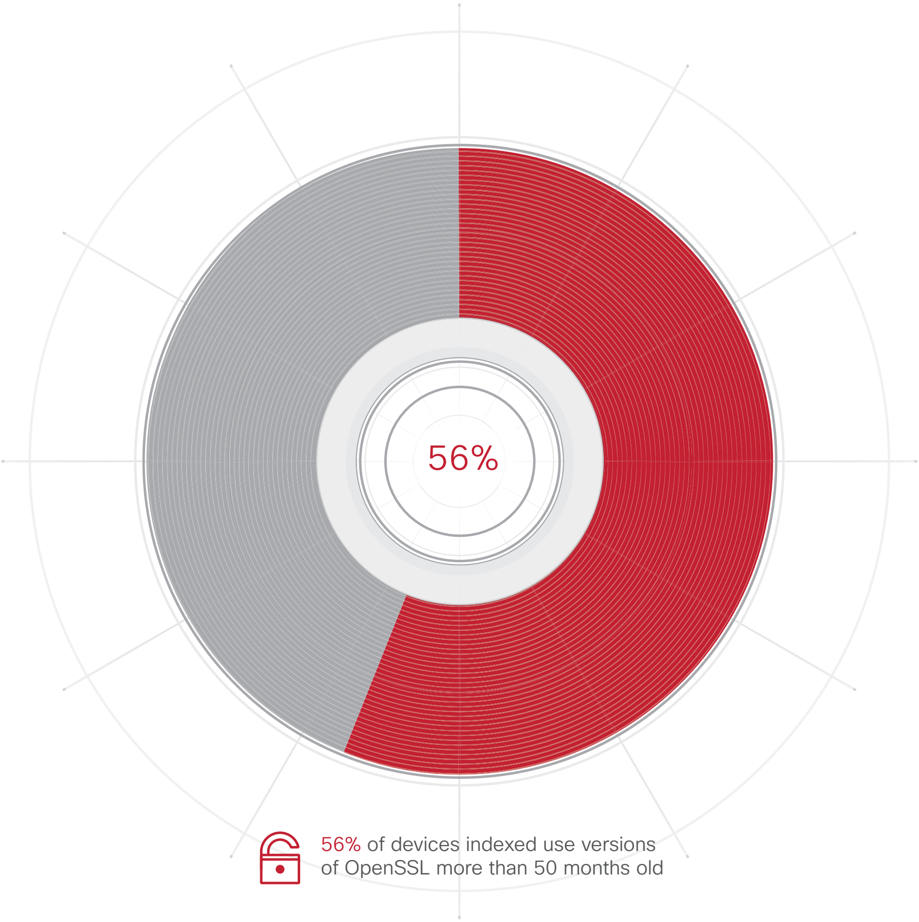
Share the report

Uncovering the Archaeology of Vulnerabilities: The Dangers of Outdated Software—and Why Patching Isn't the Only Solution

As explained in the discussion about vulnerabilities (see page 8), adversaries take the easiest path available when determining how and where their exploits will succeed. They choose products that present more attack surface opportunities; those opportunities are generally created by the use of unpatched or outdated software. For example, appliance patching remains a challenge since there are many systems still vulnerable to the SSL Poodle attack.[5] Based on observed trends, Cisco Security Research suggests that the proliferation of outdated versions of exploitable software will continue to lead to security issues of great magnitude.

Cisco Security Research used scanning engines to examine devices connected to the Internet and using OpenSSL. The team determined that 56 percent of devices surveyed used versions of OpenSSL that were more than 50 months old. This means that despite the publicity given to Heartbleed,[6] the security flaw in the handling of Transport Layer Security (TLS) discovered in 2014, and the urgent need to upgrade to the latest version of OpenSSL software to avoid such vulnerabilities, organizations are failing to ensure that they are running the latest versions. Figure 8 shows the age of OpenSSL versions.

Figure 8. OpenSSL Version Age



56% of devices indexed use versions of OpenSSL more than 50 months old

Source: Cisco Security Research

Share the report

Possible Solutions: Automatic Updates and Patching

Greater use of automatic updating may be one solution to the outdated software problem. Cisco Security Research examined data from devices that were connected online and using either the Chrome or IE browser. The data showed that 64 percent of Chrome requests originate from the latest version of that browser. As for IE users, just 10 percent of requests originated from the latest version.

Cisco Security Research suggests that the Chrome automated update system may be more successful in ensuring that as many users as possible have the most recent software version. (Also, it's possible that Chrome users are more technically proficient than IE users and thus, are more likely to update their browsers and install updates.)

When combined with the downturn in Java vulnerabilities and exploitation, the research clearly indicates that software that automatically installs its own updates seems to have an advantage in creating a safer security framework. To overcome the guaranteed eventual compromise that results from manual update processes, it may be time for organizations to accept the occasional failure and incompatibility that automatic updates represent.

Industry Vertical Risk Report: Targeting by Adversaries and Users' Careless Practices Are a Potent Combination for Companies in High-Risk Verticals

The pharmaceutical and chemical industry has emerged as the number-one high-risk vertical for web malware encounters in 2014. For the first half of the year, media and publishing held the top spot, but had edged down to second place by November. Rounding out the top five are manufacturing, transportation and shipping, and aviation, respectively. All of these verticals placed in the top five for the first half of 2014.

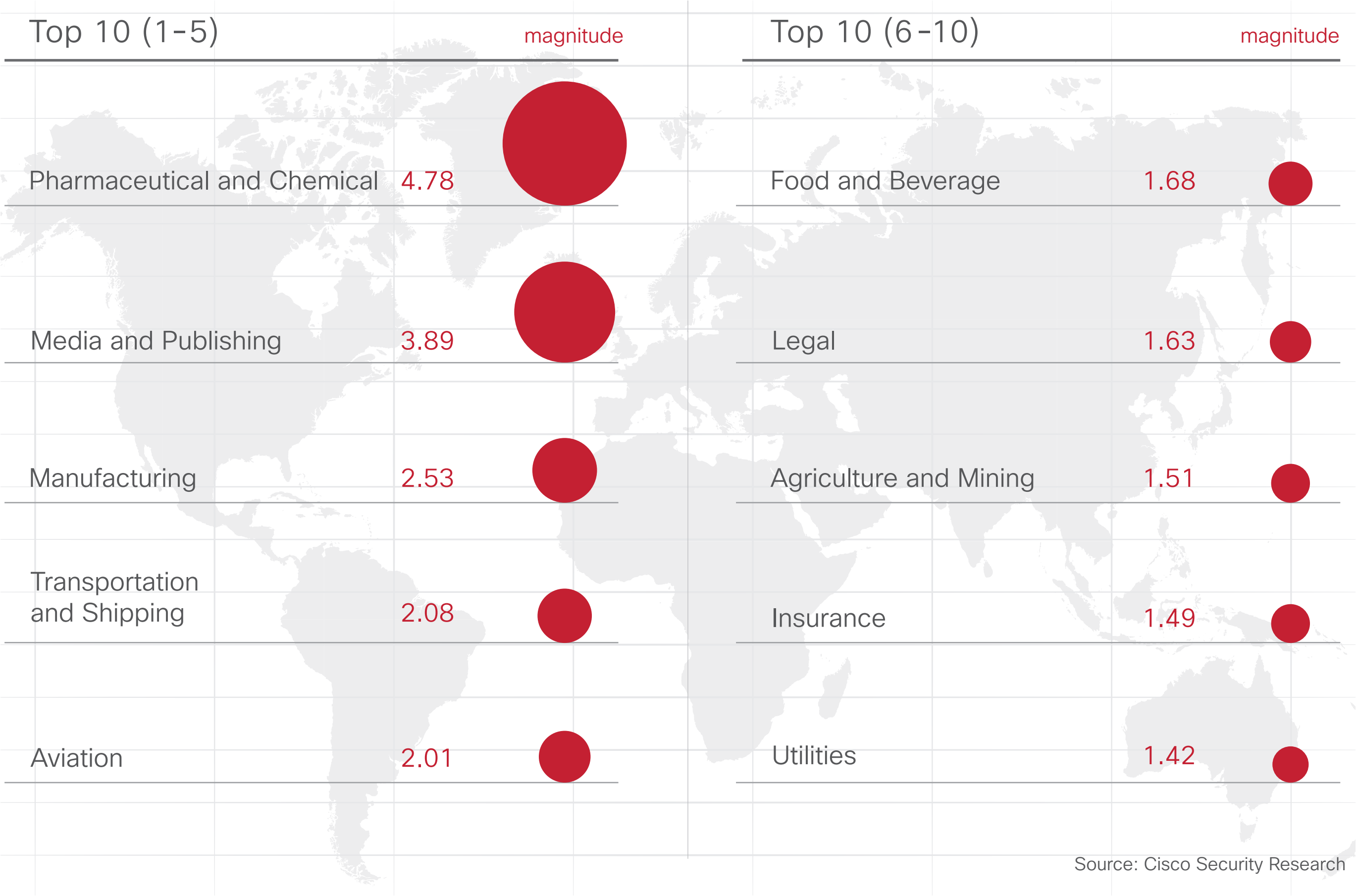
While the retail vertical might be expected to have a higher ranking on this list given recent high-profile attacks that have plagued the industry, it is malicious encounters, and not actual breaches, that are used to create the rankings.

To determine sector-specific malware encounter rates, Cisco Security Research compares the median encounter rate for all organizations that use Cisco Cloud Web Security to the median encounter rate for all companies in a specific sector that are using the service (Figure 9). An industry encounter magnitude above 1 reflects a higher than normal risk of web malware encounters, whereas a magnitude below 1 reflects a lower risk. For example, a company with a 1.7 encounter magnitude is at a 70 percent increased risk than the median. Conversely, a company with a 0.7 encounter magnitude is 30 percent below the median risk of encounter.

Encounter vs. Compromise

An "encounter" is an instance when malware is blocked. Unlike a "compromise," a user is not infected during an encounter because a binary is not downloaded.

Figure 9. Vertical Risk of Web Malware Encounters,
All Regions, January 1 – November 15, 2014



Source: Cisco Security Research

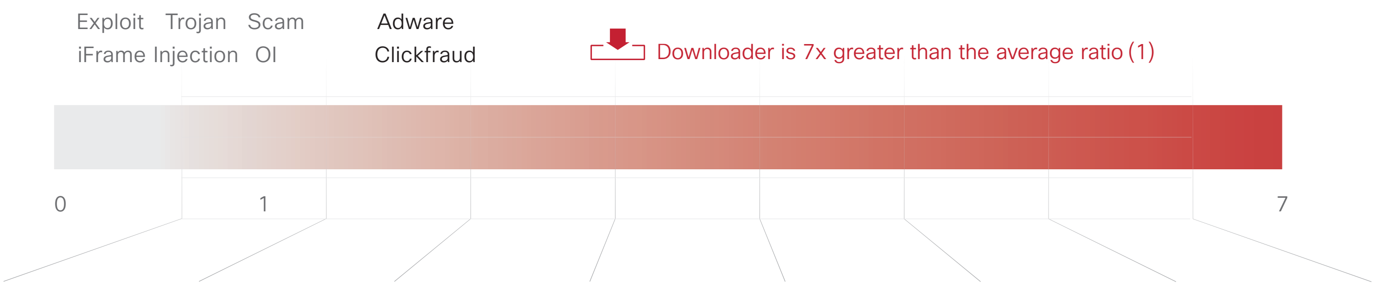
Cisco Security Research examined eight types of attack methods (Figure 10) to determine whether targeting by adversaries or how people use the web was the key factor for increasing an industry vertical's risk for malware encounters. They found a perfect storm, with the combination of targeted attack methods and careless user behavior online both having an impact on the level of risk.

To determine whether there was in fact a difference between high- and low-risk vertical user behavior, Cisco Security Research looked at four types of non-targeted attack methods users often encounter when browsing the Internet: adware, clickfraud, scam, and iframe injections. The team also looked at four types of more advanced attack methods that adversaries often employ in targeted campaigns: exploit, Trojan, OI (detection malware), and downloader.

Note: The eight attack methods have been categorized by Cisco Security Research into heuristic buckets.

Share the report

Figure 10. Web Malware Attack Methods: Comparison of the Top Four and Bottom Four High-Risk Verticals



Source: Cisco Security Research

Using the top and bottom four most malware-exposed verticals, according to Cisco Cloud Web Security data, Cisco Security Research then took the percentage of incidents for each type of attack method and created average rates for the top and bottom four verticals. The comparison shown in Figure 10 was derived by dividing the top average by the bottom average. A ratio of one indicates that the same patterns of activity are observed between the most- and least-targeted groups.

The data shows that the most high-risk industry verticals encounter sophisticated downloader attack methods at a frequency seven times higher than that of the bottom four high-risk industry verticals. This is consistent with what one would expect if targeted attack methods against the highest-risk verticals were taking place.

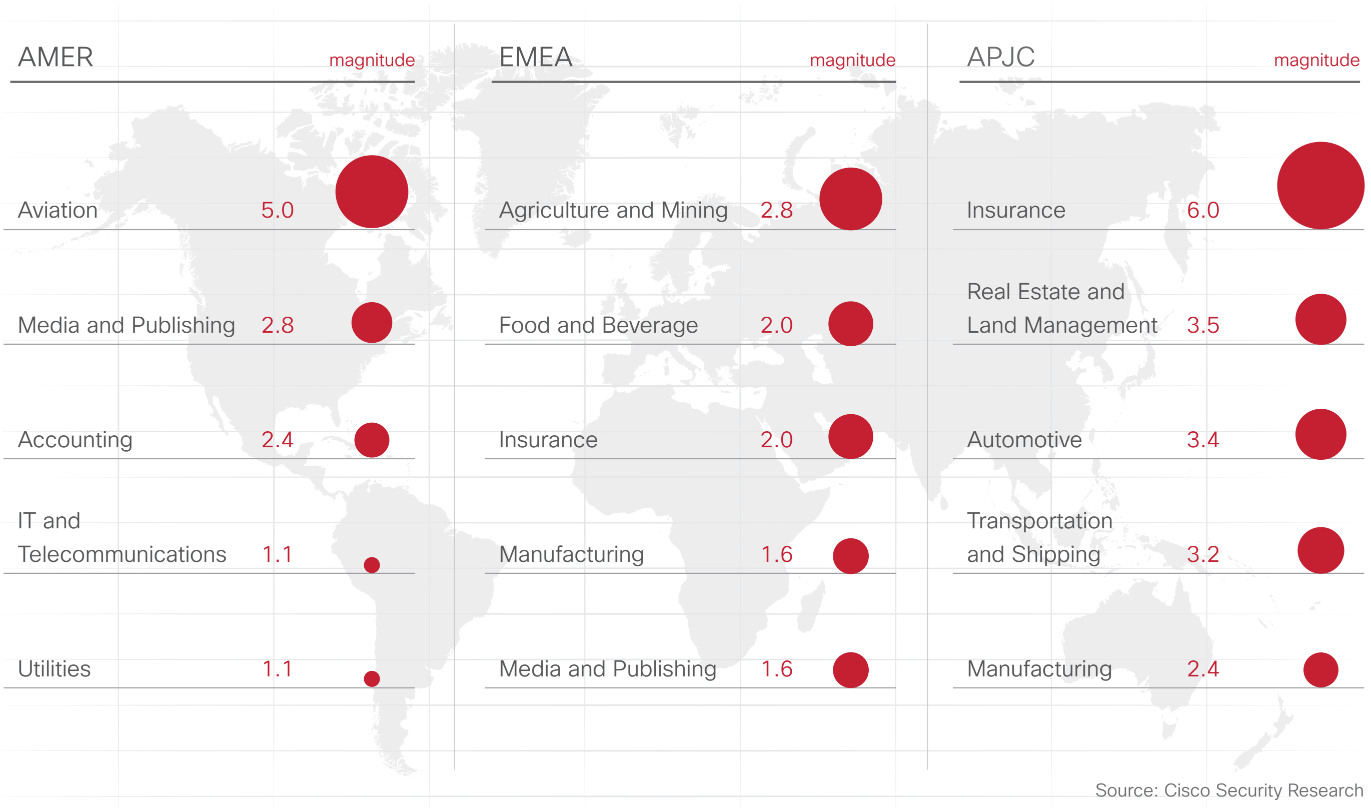
The rate of encounters with clickfraud and adware is also higher in the most-targeted and high-risk industry verticals compared to the less-targeted and lower-risk verticals. This suggests that the difference may be more complex than just targeting by malicious actors. User behavior may also be implicated in the increased exposure to malware, possibly through differences in how users engage with the Internet and their browsing habits, and are therefore contributing to the higher frequency of web malware attack method encounters in high-risk industry verticals. Also, users in industries where the quick embrace of new media is encouraged and necessary for competition and innovation are likely encountering web malware attack methods at higher rates than users in other industries, such as government, where Internet use may be more limited and/or strictly controlled.

For example, Cisco Security Research suggests that because users in the media and publishing industry are typically heavy users of the Internet, they are at risk of encountering web exploits more often than users in other industry verticals.

Note: In 2014, the media and publishing industry experienced significantly higher than normal rates of web malware encounters than previously observed by Cisco Security Research, which has been compiling this data since 2008. Users' exposure to more widespread malvertising on legitimate websites could be a contributing factor to this increase.

Share the report

Figure 11. Highest-Risk Verticals for Malware Exposure across AMER, APJC, and EMEA



Source: Cisco Security Research

Malware Encounters by Region

Following is web malware encounter risk data for high-risk industry verticals according to region. The three regions are defined as follows:

- North America, Central America, and Latin America (AMER)
- Asia-Pacific, China, Japan, and India (APJC)
- Africa, Europe, and the Middle East (EMEA)

Cisco Security Research identified the highest-risk localized industry verticals (see industries listed in Figure 11) across the world and determined that:

- Users in the insurance industry in APJC are six times more likely to be exposed to malware compared to the 12 verticals examined in all three regions. (Baseline average: 1.5.)
- Users in the aviation industry in AMER are five times more likely to be exposed to malware.
- Users in the real estate and land management industry in APJC, and users in the automotive industry in that region, are both 3.5 times more likely to be exposed to malware.
- Users in the transportation and shipping industry in APJC are 3.25 times more likely to be exposed to malware.

Cisco Security Research cites skyrocketing land and housing prices, recent natural disasters, and heavy export and manufacturing activity in APJC as factors for adversaries targeting users in that region who work in or do business with the automotive, insurance, real estate and land management, and transportation and shipping industries. Theft of customer data, intellectual property (including targeting by nation states), and air freight data are likely top motivations for targeting users in the aviation industry in AMER.

Share the report

Attack Methods for Distributing Malware, by Region

Figures 12a through 12c reveal, by region, the techniques adversaries are using most often to distribute malware. The findings in these charts are based primarily on where blocks of web malware occurred (that is, encounters), according to Cisco Cloud Web Security data, versus types of threats on the web.

During the year 2014, users in AMER were targeted primarily by malicious scripts; iframe injections were a distant second. In APJC, adversaries have been relying heavily on scams, malicious scripts, and web-based exploits over the past year to compromise users in all verticals. And in EMEA, web-based exploits are especially prevalent.

Read the Cisco Security blog post, "Threat Spotlight: Group 72," to learn about the role of Cisco Security Research in helping to identify and disrupt the activities of a threat actor group targeting high-profile organizations with high-value intellectual property in the manufacturing, industrial, aerospace, defense, and media sectors.

For details on the Remote Administration Tool (RAT) that Group 72 used to conduct cyberespionage, view this post: "Threat Spotlight: Group 72, Opening the ZxShell."

Figure 12a. Attack Method Distribution, AMER

Attack Method	Total %
Script	24.93%
iFrame Injection	17.43%
Exploit	13.63%
OI (detection malware)	10.35%
Trojan	10.06%

Source: Cisco Security Research

Figure 12b. Attack Method Distribution, APJC

Attack Method	Total %
Scam	25.26%
Script	25.04%
iFrame Injection	18.68%
OI (detection malware)	9.93%
Exploit	6.72%

Source: Cisco Security Research

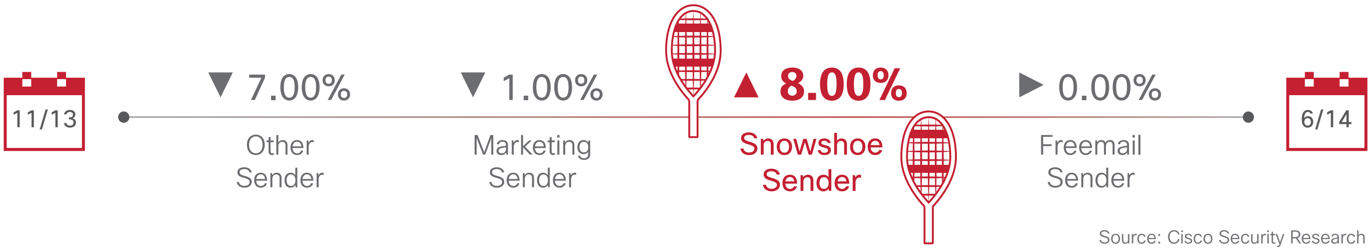
Figure 12c. Attack Method Distribution, EMEA

Attack Method	Total %
iFrame Injection	51.48%
Script	15.17%
Exploit	8.64%
Scam	7.31%
OI (detection malware)	4.16%

Source: Cisco Security Research

Share the report

Figure 13. Spam from Snowshoe Senders on the Rise



Source: Cisco Security Research

Spam Update: Spammers Adopt the "Snowshoe" Strategy

Phishing continues to prove its value to criminals as a tool for malware delivery and credential theft because users still fall prey to familiar spam tactics. Attackers have become aware that it is often easier to exploit users at the browser and email level, rather than compromising servers—which means spammers continue to innovate.

It is not uncommon to see an anti-spam system catch more than 99 percent of the spam passing through it. Most of the best anti-spam systems catch more than 99.9 percent of spam. In this environment, spammers try just about anything to evade spam filters. To ensure that spam reaches its intended audience, spammers are increasingly using these tactics to avoid detection by IP-based anti-spam reputation technologies.

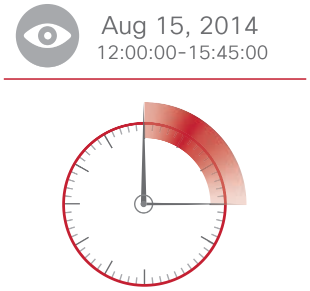
Enter snowshoe spam: The comparison is apt because snowshoes allow a person to walk over deep snow by distributing their weight over a larger surface area, thus preventing the wearer's foot from sinking. Snowshoe spam is unsolicited bulk email that is sent using a large number of IP addresses, and at a low message volume per IP address, thus preventing some spam systems from sinking the spam. Figure 13 highlights the rise in snowshoe spam from 2013 to 2014.

In a recent snowshoe spam campaign observed by Cisco Security Research, a blitz approach was used. This means the total spam campaign took place over just three hours, but at one point accounted for 10 percent of global spam traffic (Figure 14).

To learn more about snowshoe spam, see the Cisco Security blog post, "Snowshoe Spam Attack Comes and Goes in a Flurry."

The snowshoe messages examined by Cisco researchers show some standard hallmarks of spam. For example, they have misspelled subject lines such as "inovice 2921411.pdf," and include a randomly generated number. Attachments were typically PDF files containing a Trojan exploiting a vulnerability in Adobe Reader.

Figure 14. Snowshoe Spam Campaign Incident



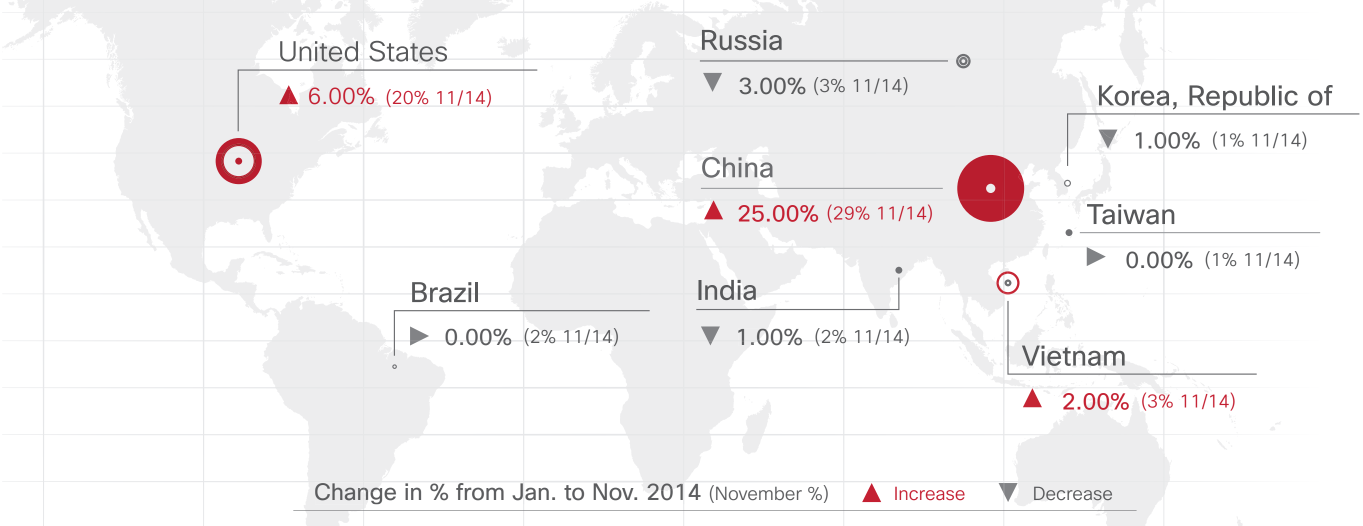
Source: Cisco Security Research

To mitigate snowshoe spam, security professionals cannot simply rely on solutions that are based on reputation, since the same messages in a campaign can originate from hundreds or even thousands of places in the case of botnet-derived campaigns. Examining other hallmarks of spam, such as email server hygiene, can provide more precise detection. In the campaigns observed by Cisco Security Research, for instance, many of the IP addresses lacked matching forward and reverse domain name systems (DNS), which is generally considered an obvious indicator that a mail server is not legitimate.

Many of these IP addresses also lacked records of sending emails prior to the start of the snowshoe campaign, further indicating that online criminals are using compromised machines to create an infrastructure for snowshoe spam.

Share the report

Figure 15. Spam Volumes by Country



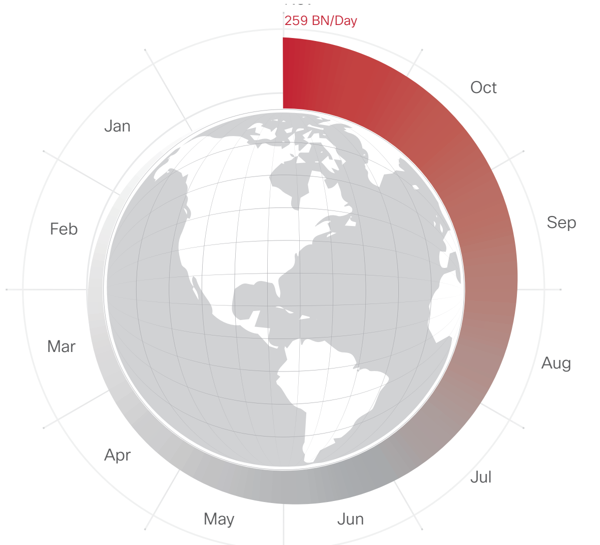
Source: Cisco Security Research

Spammers Expand Tactics to Outwit Consumers

Worldwide spam volumes are on the rise, indicating that spam is still a lucrative vector for online criminals (Figure 16). Adversaries continue to refine messages so that spam is more likely to fool recipients into clicking on dangerous links, often using social engineering tactics.

While spam volume has generally been on the decline in the United States in 2014, levels rose in other countries during the same time period (Figure 15). Cisco Security Research suggests that this indicates some malicious actors may be shifting their base of operations. The rise in spam volume in some countries may also be a sign that other regions are catching up to the United States in terms of spam production, as the country has long been a leading source of worldwide spam. Ultimately, the United States ended the year higher.

Figure 16. Worldwide Spam Volume Increase in 2014



Source: Cisco Security Research

Spear-phishing messages, a staple of online criminals for years, have evolved to the point where even experienced end users have a hard time spotting faked messages among their authentic emails. These messages, which target specific individuals with a well-crafted message, appear to come from well-known vendors or service providers from whom users commonly receive messages—for example, delivery services, online shopping sites, and music and entertainment providers. Emails with a trusted name and a logo, even if spoofed, carry more weight than the old-school spam messages touting pharmaceuticals or watches. And if the messages have a call to action that is familiar to recipients, such as a notice about a recent order, or a delivery tracking number, users will be further enticed to click on links contained in the email.

Cisco Security Research recently observed a small number of spear-phishing messages purporting to originate from Apple Inc., claiming that the recipients had downloaded a popular game for mobile iOS devices. The email subject line included a randomly generated receipt number, another seemingly authentic touch, since legitimate emails would usually contain such a number. A link in the message suggested that recipients log in and change their passwords if they had not initiated the game download, and the link redirected the user to a known phishing website.

Share the report

Spammers Morph Messages to Evade Detection

When spammers find a formula that succeeds—meaning they are able to convince users to click on links within spam, or purchase fake products—they will tweak messages so that their basic structure remains the same. But the messages are different enough that they can evade spam filters, at least for a short time. In Table 2, Cisco researchers tallied the number of times during a sample period that the spammers attempted to change message content in order to evade ongoing mitigations. The table lists those threats that required Cisco Email Security Appliance (ESA) rule changes.

Table 2. Threat Outbreak Alerts: Most Persistent Spam and Phishing Threats

IntelliShield ID		Headline	Version	Urgency	Credibility	Severity
24986	📦	Threat Outbreak Alert: Fake FedEx Shipment Notification	95	■■■■□	■■■■■	■■■□□
31819	✕	Threat Outbreak Alert: Fake Fax Message Delivery Email	88	■■■■□	■■■■■	■■■□□
30527	📷	Threat Outbreak Alert: Malicious Personal Pictures Attachment	81	■■■■□	■■■■■	■■■□□
36121	$	Threat Outbreak Alert: Fake Electronic Payment Canceled	80	■■■■□	■■■■■	■■■□□
23517	🛍	Threat Outbreak Alert: Fake Product Order Email Message	79	■■■■□	■■■■■	■■■□□
23517	$	Threat Outbreak Alert: Fake Invoice Statement Attachment	78	■■■■□	■■■■■	■■□□□
27077	$	Threat Outbreak Alert: Fake Money Transfer Notification	78	■■■■□	■■■■■	■■□□□
26690	$	Threat Outbreak Alert: Fake Bank Payment Transfer Notification	78	■■■■□	■■■■■	■■■□□

Source: Cisco Security Research

Share the report

Malvertising from Browser Add-Ons: Inflicting Slight Damage Per User to Collect Big Rewards

Cisco Security Research recently conducted in-depth analysis of a web-based threat that uses malvertising (malicious advertising) from web browser add-ons as a medium for distributing malware and unwanted applications. The group discovered that the threat has strong characteristics that resemble the behavior of a botnet. Through the team's research, which included the examination of the activity of more than 800,000 users at 70 companies from January 1 through November 30, 2014, Cisco Security Research measured the overall size of the threat and corroborated the intention and structure.

The analysis revealed that this family of browser add-ons is far more extensive than expected and that the malware creators are using a combination of highly sophisticated, professionally written code and a refined business model to keep their malware in profitable operation for the long term. In other words, full control over the targeted host is not necessary for successful monetization. This leads to increased prevalence of malware deliberately engineered for lower impact on the affected host, and optimized for long-term monetization over a large affected population.

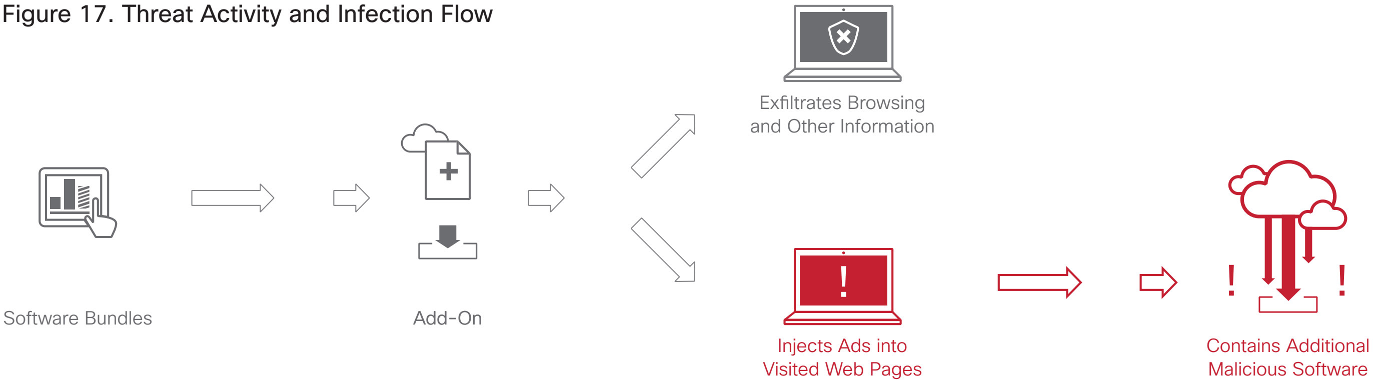
Compromised users are infected with these malicious browser add-ons through the installation of bundled software (software distributed with another software package or product) and usually without clear user consent. Applications such as PDF tools or video players downloaded from untrusted sources are installed knowingly by users believing they are legitimate. The applications can be "bundled" with unwanted and malicious software. This approach of distributing malware follows a pay-per-install (PPI) monetization scheme, in which the publisher gets paid for every installation of software bundled in the original application.

Many users inherently trust add-ons or simply view them as benign, which is why this approach to malware distribution is proving successful for malicious actors. This method of distributing malware allows adversaries to decrease their reliance on other techniques, such as exploit kits, that may be more detectable. (See "Web Exploits: For Exploit Kit Authors, Holding the Top Spot May Not Mean You're the Best," page 7.)

Cisco Security Research observed that the web traffic generated by this browser add-on family has specific characteristics, and can be identified by two well-defined patterns. The query string usually contains encoded data, in which information such as the add-on name and the URL the user previously visited (including intranet links), is exfiltrated.

During its analysis, Cisco Security Research found more than 4000 different add-on names, including PassShow, Bettersurf, Bettermarkit, and associated SHAs (bee4b83970ffa8346f0e791be92555702154348c14bd8 a1048abaf5b3ca049e35167317272539fa0dece3ac1a60 10c7a936be8cbf70c09e547e0973ef21718e5). Because more than one add-on name may be used per installation, the malware is very difficult to track (Figure 17).

Figure 17. Threat Activity and Infection Flow


Software Bundles
Add-On
Exfiltrates Browsing and Other Information
Injects Ads into Visited Web Pages
Contains Additional Malicious Software

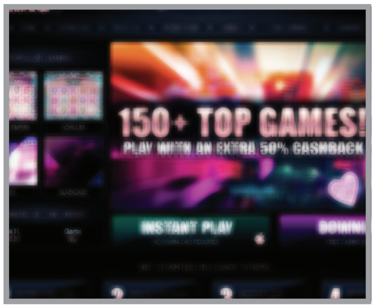
Source: Cisco Security Research

Share the report

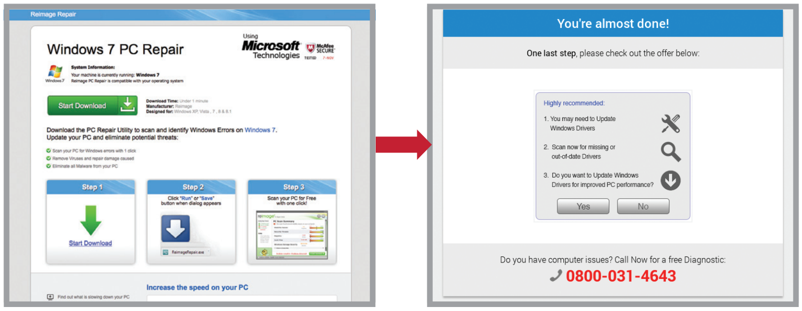
Malware Detects OS Types, Serves Up Appropriate Exploits

Cisco security researchers observed that the malicious add-ons they analyzed will display a certain type of advertising depending on the browser "fingerprint" of a user. Injected ads for Linux users were usually about online gaming sites. Users who had Microsoft IE installed were redirected to ads that lead to the download of seemingly legitimate software, which actually turns out to be malicious.

Linux



Microsoft IE


Reimage Repair

Windows 7 PC Repair

Using Microsoft Technologies

McAfee SECURE TESTED 7-NOV

System Information:
Your machine is currently running: Windows 7
Reimage PC Repair is compatible with your operating system

Download Time: Under 1 minute
Manufacturer: Reimage
Designed for: Windows XP, Vista , 7 , 8 & 8.1

Download the PC Repair Utility to scan and identify Windows Errors on Windows 7.
Update your PC and eliminate potential threats:

- Scan your PC for Windows errors with 1 click
- Remove Viruses and repair damage caused
- Eliminate all Malware from your PC

Step 1 Start Download

Step 2 Click "Run" or "Save" button when dialog appears

Step 3 Scan your PC for Free with one click!

Increase the speed on your PC

Find out what is slowing down your PC

You're almost done!

One last step, please check out the offer below:

Highly recommended:

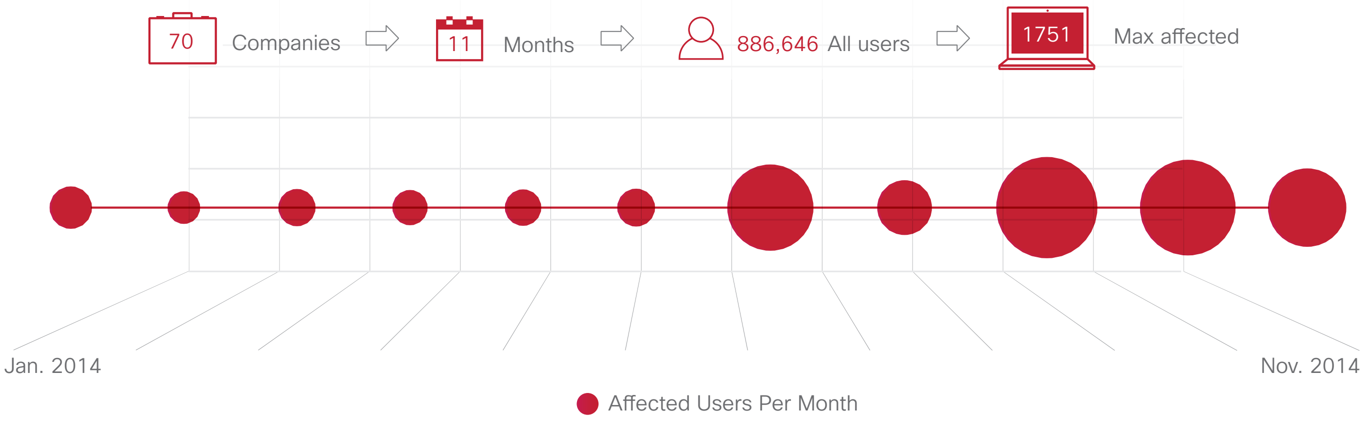
1. You may need to Update Windows Drivers
2. Scan now for missing or out-of-date Drivers
3. Do you want to Update Windows Drivers for improved PC performance?

Do you have computer issues? Call Now for a free Diagnostic:
☎ 0800-031-4643

Based on analysis of 11 months of user activity at 70 companies, the number of users affected by this threat has been rising. In January, 711 users were affected, but in the second half of the year the number of affected users went above 1000, with a peak in September, of 1751 (Figure 18). One of the reasons for the significant spike in September and October could be the increase in online activity, with people back to work after summer vacations.

Through research, Cisco security experts learned that adversaries are employing several different servers to support their malware campaigns. This likely means that either one cybercriminal organization skilled at keeping its activities segmented is responsible for the threat, or one "technology provider" is selling its product to several groups. Regardless, whoever is responsible for distributing the malware appears to be attempting to create a botnet of substantial size.

Figure 18. Number of Affected Users Per Month, Jan. through Nov. 2014



Source: Cisco Security Research

Cisco Security Research also found more than 500 unique domains associated with this threat; 24 of them are ranked on Alexa below the top 1 million domains. Many are also relatively highly ranked domains (Figure 19). This means they are popular domains, yet very dangerous for users to visit due to the risk of compromise.

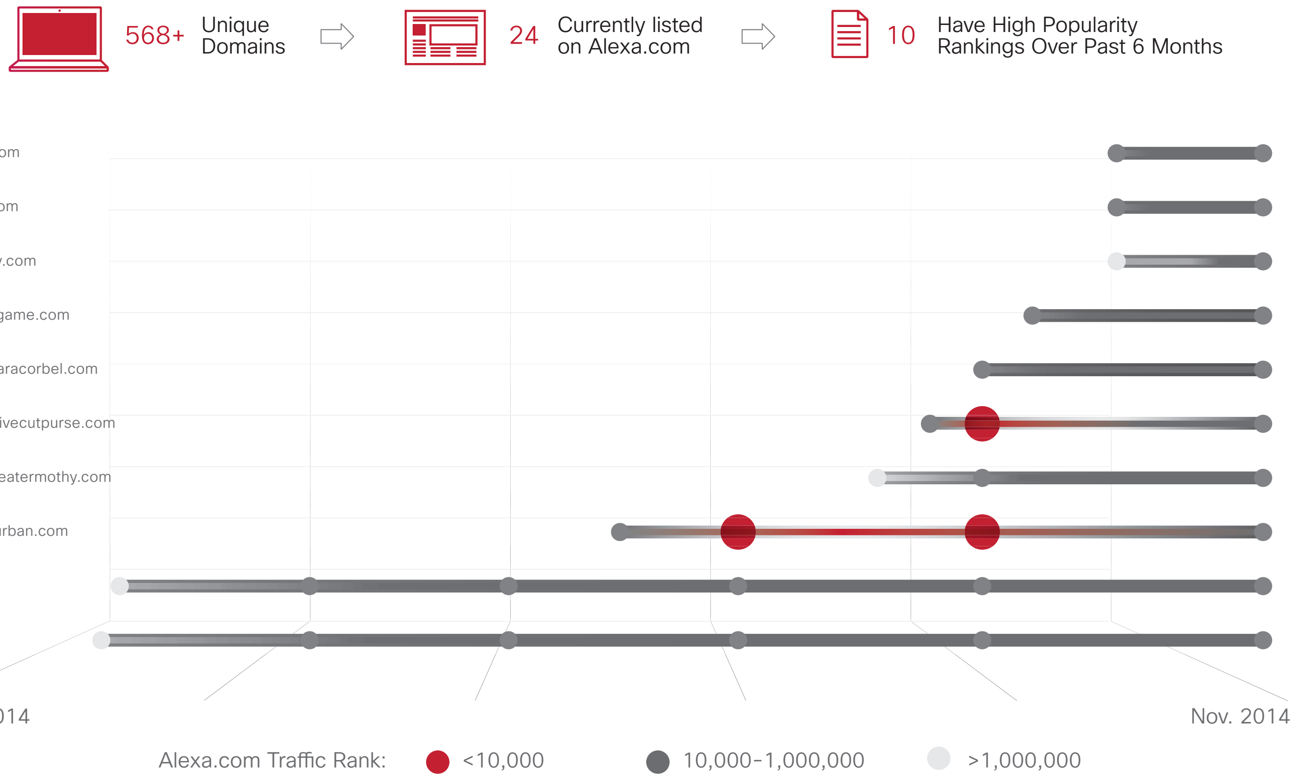
Some of the domains have been active for more than a year, but most have a much shorter lifecycle—only a few weeks, in many cases (Figure 19). All of the domains share one characteristic: They become popular very quickly.

Tips for Prevention and Remediation

To avoid being compromised by the browser ad-don scheme, or to address an existing infection, users should apply the following tips:

- Download applications from trusted sources
- Unselect unwanted software in bundle installs
- Use threat analytics, sandboxing technologies, and web security technologies to help prevent and detect this type of threat
- Manually remove add-ons if possible; also, use antispyware tools to clean up unwanted programs

Figure 19. Popular Domains Used for Malvertising in the Browser Add-On Scheme, Rated on Alexa



Source: Cisco Security Research

Share the report

2. Cisco Security Capabilities Benchmark Study

To gauge perceptions of security professionals on the state of security in their organizations, Cisco asked chief information security officers (CISOs) and security operations (SecOps) managers in several countries and at organizations of different sizes about their security resources and procedures. The *Cisco Security Capabilities and Benchmark Study,* completed in October 2014, offers insights on the sophistication level of security operations, and security practices currently in use.

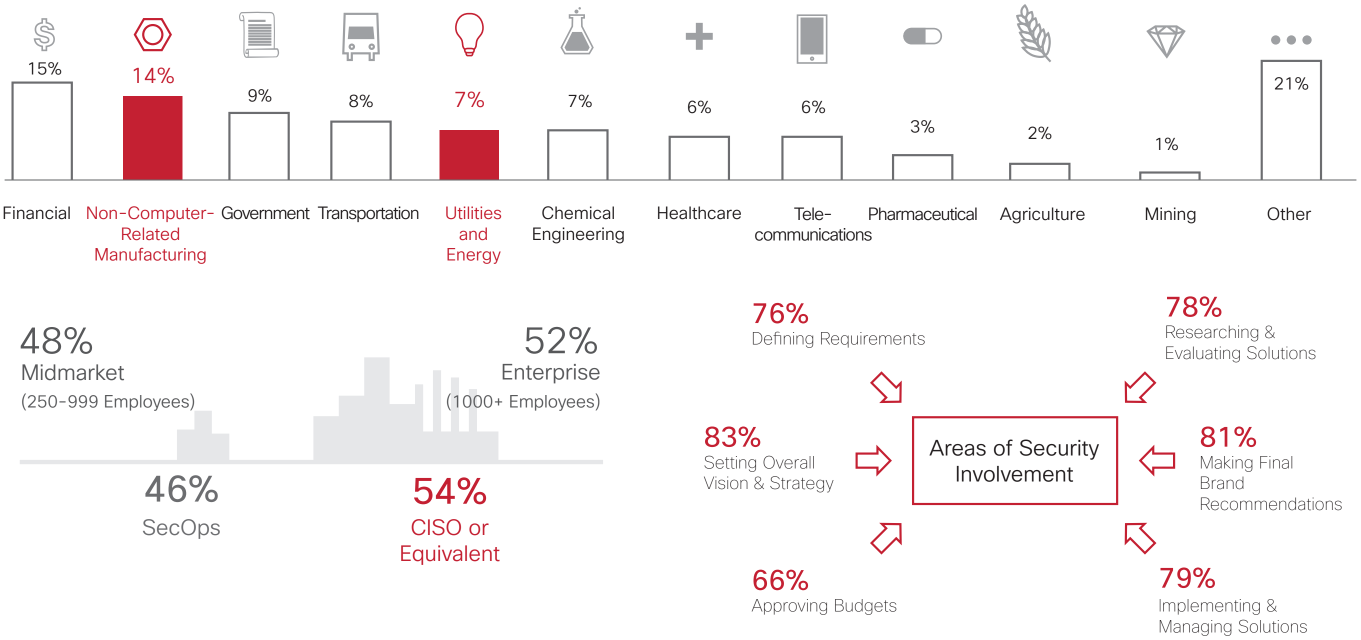
Cisco Security Capabilities: How Well Do Organizations Measure Up?

How do enterprise security professionals view their organizations' readiness to handle security breaches? The answer may depend on the role they play within an organization, and which industry they work in, according to the new Cisco Security Capabilities Benchmark Study.

Figure 20 shows the responses of professionals by industry and company size. Non-computer-related manufacturers and utility/energy respondents report the highest levels of security involvement and knowledge.

N (number of respondents) = 1738

Figure 20. Respondent Profiles and Security Breach Readiness



Source: *Cisco Security Capabilities Benchmark Study*

The study surveyed CISOs and SecOps managers to learn about the resources their companies are devoting to cybersecurity; their security operations, policies, and procedures; and the sophistication level of their cybersecurity operations. The good news from the survey is that a majority of security professionals believe they have the tools and processes in place to maintain security effectively. However, CISOs are notably more optimistic than their SecOps colleagues about the state of their security. For example, 62 percent of CISOs said they strongly agree that security processes in their organization are clear and well understood, compared to only 48 percent of SecOps managers. CISOs also view their security processes in a more favorable light. Fifty-nine percent of those surveyed strongly agree that these processes are optimized, and that they now focus on process improvement, compared to 46 percent of SecOps managers.

Why the gap in confidence levels? It's likely due to the fact that CISOs are more removed from day-to-day security activities, whereas SecOps staff are working closely to resolve both major and minor security incidents. A CISO of a very large organization might not realize that a thousand machines are infected by malware in a typical day, whereas the SecOps manager would have devoted much more time to mitigating the infection, hence his or her less optimistic outlook on organizational security.

In addition, CISOs may be setting policies, such as blocking access to social media, which give them the illusion of tighter, more impenetrable security defenses. However, by shutting down such channels completely, security teams may lack knowledge or experience of the threats that still exist just outside their networks.

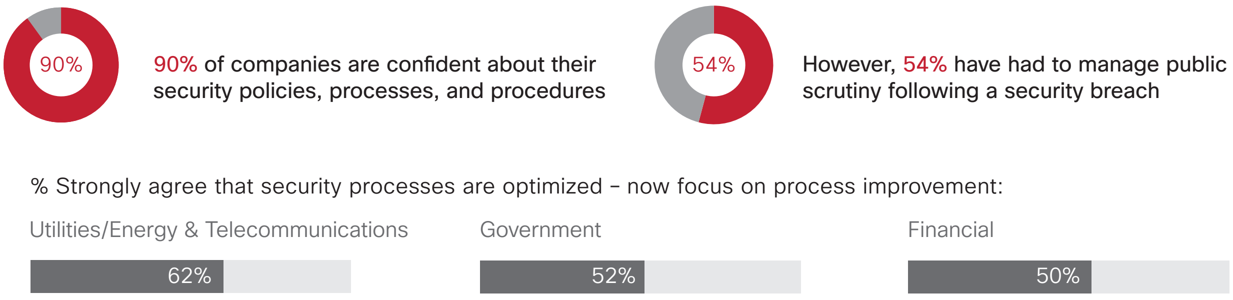
Another gap in confidence appeared when respondents were asked about their confidence in their organizational security policies. Both CISOs and SecOps managers show high levels of confidence in policies (see Figure 21); yet they have less confidence in their abilities to scope and contain compromises (see Figure 28).

A similar gap appeared when respondents were asked about their security controls: Nearly all respondents said they had good security controls, but about one-quarter perceive their security tools to be only “somewhat” rather than “very” or “extremely” effective (see Figure 29).

Confidence in security processes and practices also seems to vary by industry. CISOs and SecOps managers for utility/energy companies and telecommunications businesses seem to be the most confident, while government, financial services, pharmaceuticals, and healthcare organizations seem less confident. For instance, 62 percent of telecommunications and utility/energy security executives strongly agree that their security processes are optimized, compared to 50 percent of those working in financial services and 52 percent in government.

Utilities/energy and telecommunications security professionals seem to be the most sophisticated in their security practices, while government and financial services organizations seem less sophisticated. Utility and energy organizations tend to have well-documented processes and procedures for incident tracking. However, this does not necessarily mean they are more secure than organizations in other industries.

Figure 21. Key Findings by Industry and Job Title



90% of companies are confident about their security policies, processes, and procedures

However, 54% have had to manage public scrutiny following a security breach

% Strongly agree that security processes are optimized – now focus on process improvement:

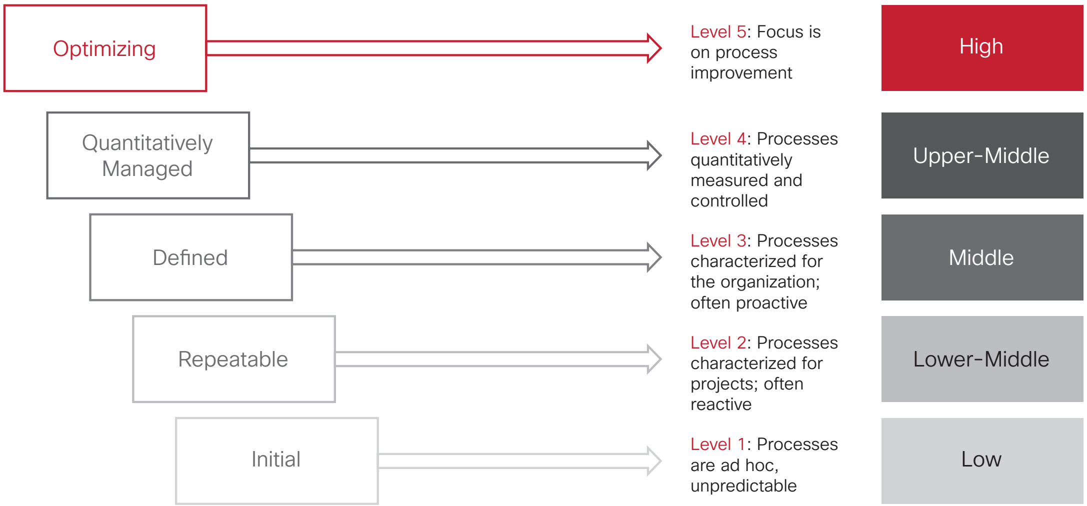
Few differences emerge between enterprise and midmarket organizations, indicating that number of employees alone has little to do with security sophistication.

Source: *Cisco Security Capabilities Benchmark Study*

Share the report

Figure 22. Mapping Sophistication Levels to Current Sample

Cisco explored several options for sample segmentation before selecting a five-segment solution based on a series of questions targeting security processes. The five-segment solution maps fairly closely to the Capability Maturity Model Integration (CMMI).


Optimizing
Quantitatively Managed
Defined
Repeatable
Initial
Level 5: Focus is on process improvement
Level 4: Processes quantitatively measured and controlled
Level 3: Processes characterized for the organization; often proactive
Level 2: Processes characterized for projects; often reactive
Level 1: Processes are ad hoc, unpredictable
High
Upper-Middle
Middle
Lower-Middle
Low

Source: *Cisco Security Capabilities Benchmark Study*

Signs of Security Sophistication

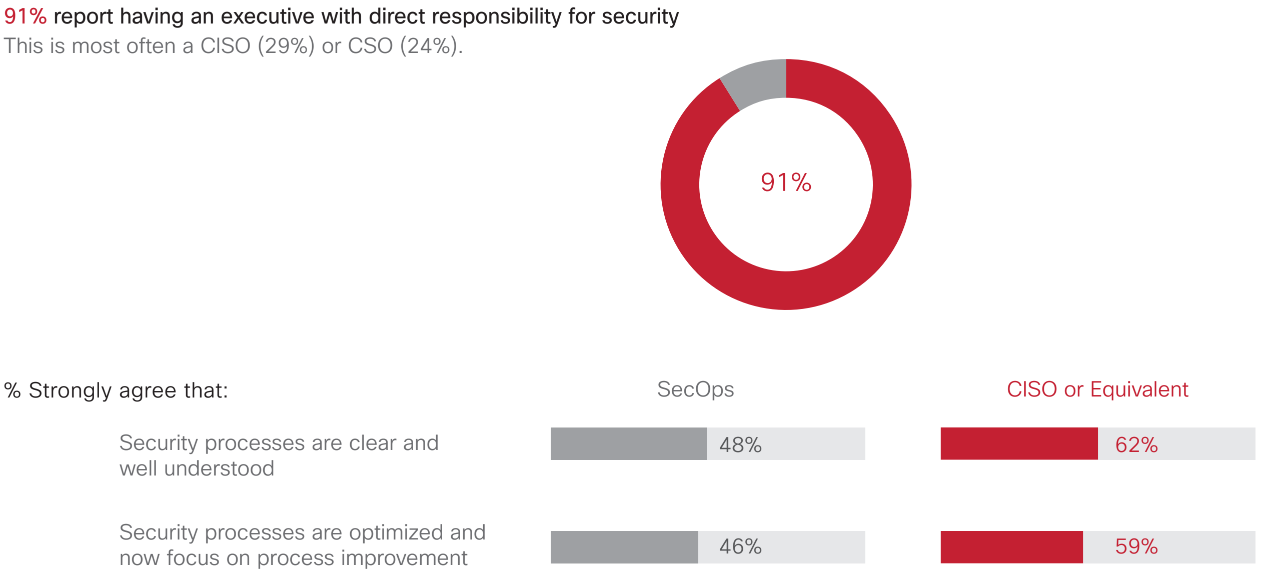
The *Cisco Security Capabilities Benchmark Study* also highlighted the hallmarks of organizations that are more sophisticated in their security posture than others. These hallmarks include:

- Executive leadership that prioritizes security
- Clear, well-documented policies and procedures
- Integrated tools that work together

Ninety-one percent of respondents from sophisticated companies strongly agree that company executives consider security a high priority, while only 22 percent of respondents from the least-sophisticated companies agree with this statement. In addition, 88 percent of respondents from sophisticated companies strongly agree that security processes are clear and understood, compared to 0 percent of respondents from the least-sophisticated companies.

Share the report

Figure 23. Key Findings on Security Leadership Within Organizations



CISOs (and equivalent) are more optimistic than SecOps managers about the state of security in their companies, perhaps because they're further from day-to-day realities.

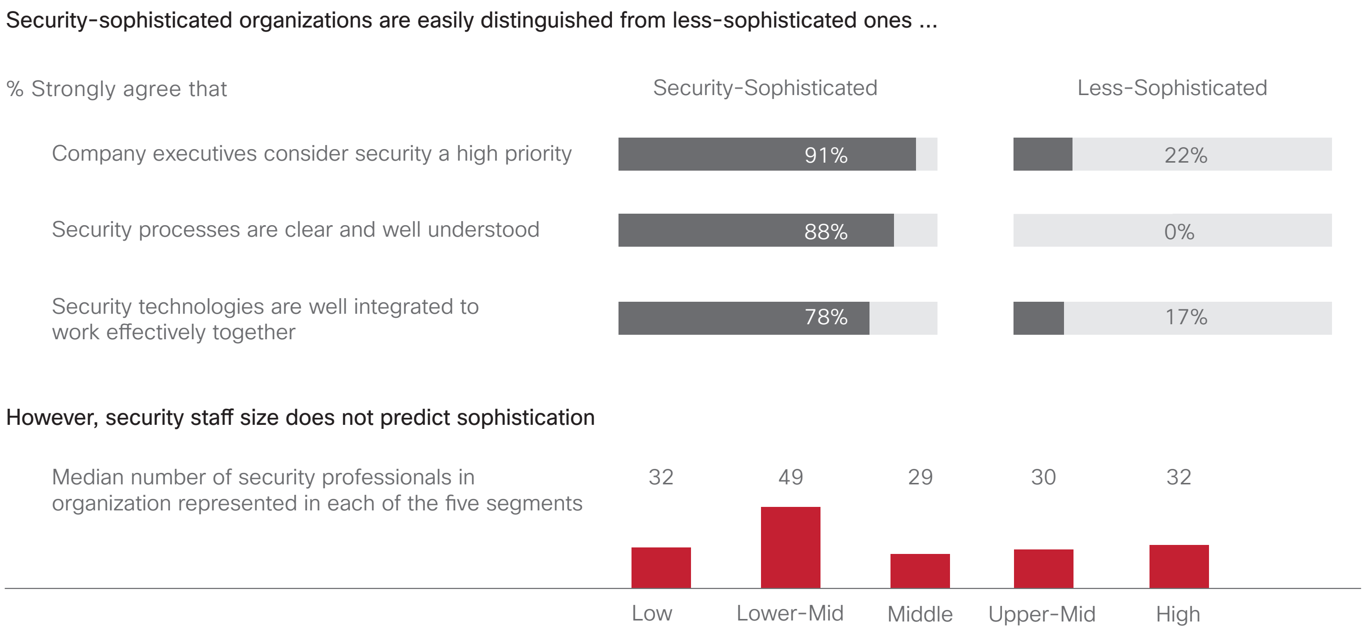
Source: *Cisco Security Capabilities Benchmark Study*

Figure 23 shows that 91 percent of respondents report having an executive with direct responsibility for security, most often a CISO or a chief security officer (CSO). The high level of organizations with a security point person is encouraging: Without security leadership, processes are less defined, communicated, and enforced. It is likely that recent high-profile security breaches have spurred on organizations to carve out a place for security management in their executive ranks.

Seventy-eight percent of respondents from more sophisticated companies strongly agree that security technologies are well integrated to work effectively together, compared to 17 percent of respondents from the least-sophisticated companies.

The positive news for organizations hoping to boost the sophistication of their security processes is that assembling a large team of hard-to-find security talent isn't necessarily a requirement. In the least-sophisticated organizations, the median number of security professionals is 32; in those with the highest levels of sophistication, the median number of security staff is also 32. Therefore, employing more people does not seem to directly correlate to better management of security processes. A better approach to staffing security personnel would be to find an optimal ratio of security staff to the number of overall employees in the company.

Figure 24. Key Findings on Security Prioritization



Source: *Cisco Security Capabilities Benchmark Study*

Figure 24 reveals that less-sophisticated security organizations generally do not believe that executives consider security a high priority, nor do they believe that security processes are clear and well understood.

In comparing the security sophistication level of organizations by country, there's more good news: Highly sophisticated organizations are the majority in every segment. However, respondents in some countries appear to have a more positive view of their own security stance than the outside world does. Overly confident perceptions from respondents in some countries may be due in part to core social values of a culture, such as the need to present one's self—and thus, one's organization—in a positive light.

Beware of Overconfidence

While CISOs and SecOps managers are showing confidence in their security operations, they also indicate that they do not use standard tools that can help thwart security breaches. Less than 50 percent of respondents use the following tools:

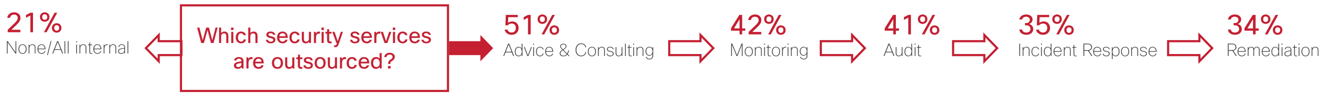
- Identity administration or user provisioning
- Patching and configuration
- Penetration testing
- Endpoint forensics
- Vulnerability scanning

Share the report

Organization Security Resources

Figure 25. Number of Dedicated Security Professionals Within Organizations

Organizations have an average of 123 professionals devoted to security. Government organizations are most likely to outsource their security services.



21% None/All internal

Which security services are outsourced?

51% Advice & Consulting

42% Monitoring

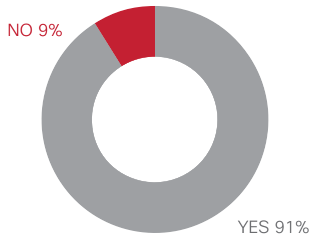
41% Audit

35% Incident Response

34% Remediation

Security Resource Snapshot

Does your organization have a security incident response team?

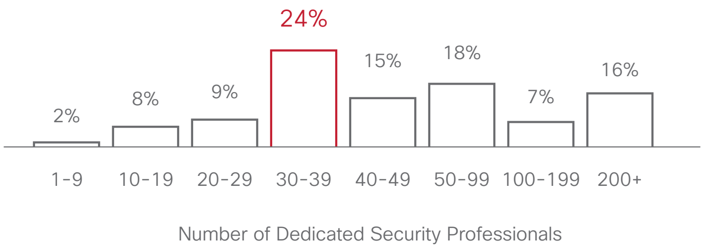


Average number of professionals dedicated to security

123

Average percentage of time spent on security-related tasks

63%



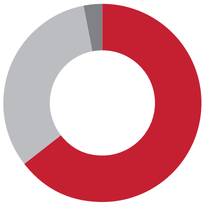
Government appears to outsource more security services than other industry groups.

Source: *Cisco Security Capabilities Benchmark Study*

Figure 26. Security Technologies Used in Organizations

About two-thirds of respondents say that their security technologies are up to date and frequently updated.

How would you describe your security infrastructure? Base: n=1738



64% Our security infrastructure is very up to date, and is constantly upgraded with the best technologies available.

33% We replace or upgrade our security technologies on a regular cadence, but aren't equipped with the latest-and-greatest tools

3% We replace or upgrade our security technologies only when old ones no longer work or are obsolete, or when we identify completely new needs.

A significantly higher proportion of **CISOs (70%)** say their organization's infrastructure is very up to date, compared with **SecOps managers (57%).**

Telecommunications companies are most likely to say their security infrastructure is kept up to date.

Source: *Cisco Security Capabilities Benchmark Study*

Figure 27. Security Threat Defenses Used by Organizations

Various security threat defenses used by organizations in 2014.

	Security Threat Defenses Used by Organization		Defenses Administered Through Cloud-Based Services	
	SecOps n=797	CISO n=941	SecOps n=759	CISO n=887
Network security, firewalls/intrusion prevention	57%	64%	30%	39%
Web security	56%	62%	33%	41%
Email/messaging security	53%	58%	33%	41%
Data loss prevention	55%	55%	–	–
Encryption/privacy/data protection	52%	55%	–	–
Access control/authorization	55%	52%	24%	24%
Authentication	54%	51%	24%	22%
Mobility security	48%	54%	24%	32%
Secured wireless	47%	52%	22%	30%
Endpoint protection/anti-malware	45%	52%	24%	27%
Vulnerability scanning	44%	51%	24%	26%
VPN	49%	46%	25%	27%
Identity administration/user provisioning	43%	47%	16%	23%
Security Information and Event Management (SIEM)	39%	46%	–	–
Network forensics	41%	43%	–	–
Patching and configuration	38%	40%	–	–
Penetration testing	39%	37%	20%	19%
DDoS defense	35%	37%	–	–
Endpoint forensics	29%	33%	–	–

Security respondents who use security threat defenses; n=1646

Thirteen percent of respondents say none of the security threat defenses used are administered through cloud-based services. This is especially true for those in the healthcare, financial services, and pharmaceutical industries.

Source: *Cisco Security Capabilities Benchmark Study*

Share the report

Organization Security Policies, Procedures and Operations

Figure 28. Confidence Levels in Organizational Security Policies and Organizational Abilities to Contain Compromises

While organizations appear to have confidence in their organizational security policies, they show significantly less confidence in their abilities to scope and contain compromises.

Confidence levels in organizational security policies

Security Policies n=1738	SecOps n=797			CISO n=941		
	Disagree	Agree	Strongly Agree	Disagree	Agree	Strongly Agree
Information assets are inventoried and clearly classified	11%	40%	49%	4%	38%	58%
We do an excellent job of managing HR security	9%	45%	46%	4%	36%	60%
Computer facilities within my organization are well protected	10%	39%	51%	4%	34%	62%
Technical security controls in systems and networks are well managed	6%	41%	53%	3%	31%	66%
Access rights to networks, systems, applications, functions, and data are appropriately controlled	8%	35%	57%	4%	32%	64%
We do a good job of building security into systems and applications	10%	38%	52%	4%	32%	64%
We do a good job of building security into our procedures for acquiring, developing, and maintaining systems	9%	41%	50%	4%	35%	61%

Confidence levels in organizational abilities to contain compromises

Security Operationalization n=1738	SecOps n=797			CISO n=941		
	Disagree	Agree	Strongly Agree	Disagree	Agree	Strongly Agree
We review and improve our security practices regularly, formally, and strategically over time	7%	42%	51%	3%	36%	61%
We have tools in place to enable us to review and provide feedback regarding the capabilities of our security practice	10%	41%	49%	4%	39%	57%
We routinely and systematically investigate security incidents	11%	40%	49%	3%	37%	60%
We can increase security controls on high-value assets should circumstances require	10%	43%	47%	3%	38%	59%
We regularly review connection activity on the network to ensure that security measures are working as intended	8%	39%	53%	4%	33%	63%
Our threat detection and blocking capabilities are kept up to date	9%	38%	53%	3%	36%	61%
Our security technologies are well integrated to work effectively together	9%	40%	51%	3%	37%	60%
Security is well integrated into our organization's goals and business capabilities	10%	39%	51%	2%	34%	64%
It is easy to determine the scope of a compromise, contain it, and remediate from exploits	15%	44%	41%	8%	42%	50%

More midmarket respondents strongly agree that they "review and improve security practices regularly, formally, and strategically over time" compared to enterprise respondents.

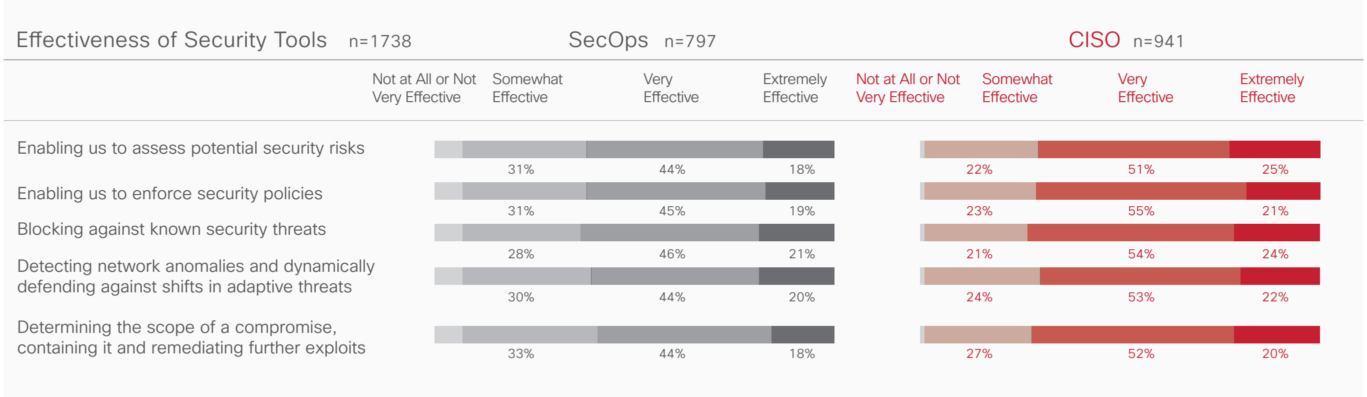
Source: *Cisco Security Capabilities Benchmark Study*

Figure 29. Respondent Beliefs About Company Security Controls and Organizational Security Tools

While security professionals believe their organizations have good security controls, about a quarter of respondents perceive their security tools to be only somewhat effective.

Security Controls n=1738	SecOps n=797			CISO n=941		
	Disagree	Agree	Strongly Agree	Disagree	Agree	Strongly Agree
We follow a standardized incident response practice such as RFC2350, ISO/IEC 27035:2011, or U.S. certification	15%	42%	43%	6%	40%	54%
We have effective processes for interpreting and prioritizing incoming incident reports and understanding them	11%	46%	43%	4%	39%	57%
We have good systems for verifying that security incidents actually occurred	11%	41%	48%	4%	36%	60%
We have a good system for categorizing incident-related information	10%	43%	47%	4%	37%	59%
We do a good job of notifying and collaborating with stakeholders about security incidents	10%	46%	44%	3%	40%	57%
We have well-documented processes and procedures for incident response and tracking	9%	40%	51%	4%	35%	61%
Cyber risk assessments are routinely incorporated into our overall risk assessment process	10%	37%	53%	4%	36%	60%

Significantly more utilities/energy respondents strongly agree with the statement "we have well-documented processes and procedures for incident response and tracking" than professionals from most all other industries.



Security professionals in the transportation industry express less confidence in their organization's ability to detect and defend against known security threats.

Source: *Cisco Security Capabilities Benchmark Study*

Share the report

Figure 30. Processes Used to Analyze Compromised Systems and Eliminate Causes of Security Incidences

Security professionals are most likely to use firewall logs to analyze compromises, even though these logs do not usually contain high-quality data or context for the information. For better analysis of compromises, security professionals should view IDS and IPS logs, proxy, host-based intrusion prevention systems (HIPS), application logs, and NetFlow regularly.

It is also surprising to see that "Correlated Event/Log Analysis" was lower on the list of tools used to analyze compromises. It may mean that the respondents are not correlating data or linking sources of data together, which can help provide more in-depth analysis of a security event.

Processes to Analyze Compromised Systems	SecOps	CISO
	n=797	n=941
Firewall log	59%	62%
System log analysis	58%	60%
Malware or file regression analysis	51%	58%
Network flow analysis	51%	54%
Registry analysis	48%	51%
Full packet capture analysis	44%	48%
Correlated event/log analysis	40%	44%
Memory forensics	39%	43%
Disk forensics	38%	41%
Indicators of Compromise (IOC) detection	38%	38%
External [or third-party] incident response/analysis teams	36%	38%

Government respondents tend to report using more processes for analyzing compromised systems than respondents from most other industries.

Processes to Eliminate Cause of Security Incidents	SecOps	CISO
	n=797	n=941
Quarantine or remove malicious application	55%	60%
Root cause analysis	55%	56%
Stop communication of malicious software	51%	55%
Additional monitoring	51%	53%
Policy updates	50%	51%
Stop communication of compromised application	47%	49%
Long-term fix development	46%	48%
Re-image system to previous state	43%	47%

CISOs' and SecOps' responses are consistent, with the exception of stop communication of malicious software.

Source: *Cisco Security Capabilities Benchmark Study*

Figure 31. CISOs and SecOps Responses on Post-Incident Controls

More CISOs report implementing additional, post-incident controls than do security operations professionals.

Processes to Restore Affected Systems	SecOps	CISO
	n=797	n=941
Implement additional or new detections and controls, based on identified weaknesses post-incident	55%	65%
Patch and update applications deemed vulnerable	59%	60%
Restore from a pre-incident backup	53%	60%
Differential restoration	53%	58%
Gold image restoration	33%	36%

Telecommunications and utilities/energy respondents say they utilize gold image restoration more than other industries.

Figure 32. Who Is Notified of Security Incidents

Operations staff and technology partners are most likely to be notified of security incidents through more formal processes.

Groups Notified in the Event of an Incident	SecOps	CISO
	n=797	n=941
Operations	44%	48%
Technology partners	42%	47%
Engineering	38%	37%
Human resources	37%	35%
Legal	37%	35%
All employees	38%	33%
Manufacturing	31%	36%
Business partners	31%	33%
Marketing	30%	31%
Public relations	30%	27%
External authorities	25%	20%

Government agencies are significantly more likely to have clearly defined notification processes with more constituent groups than other industries.

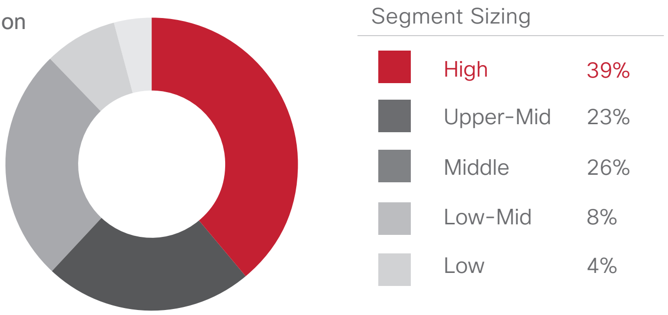
Source: *Cisco Security Capabilities Benchmark Study*

Organization Security Sophistication

Figure 33. Sophistication of Security Processes

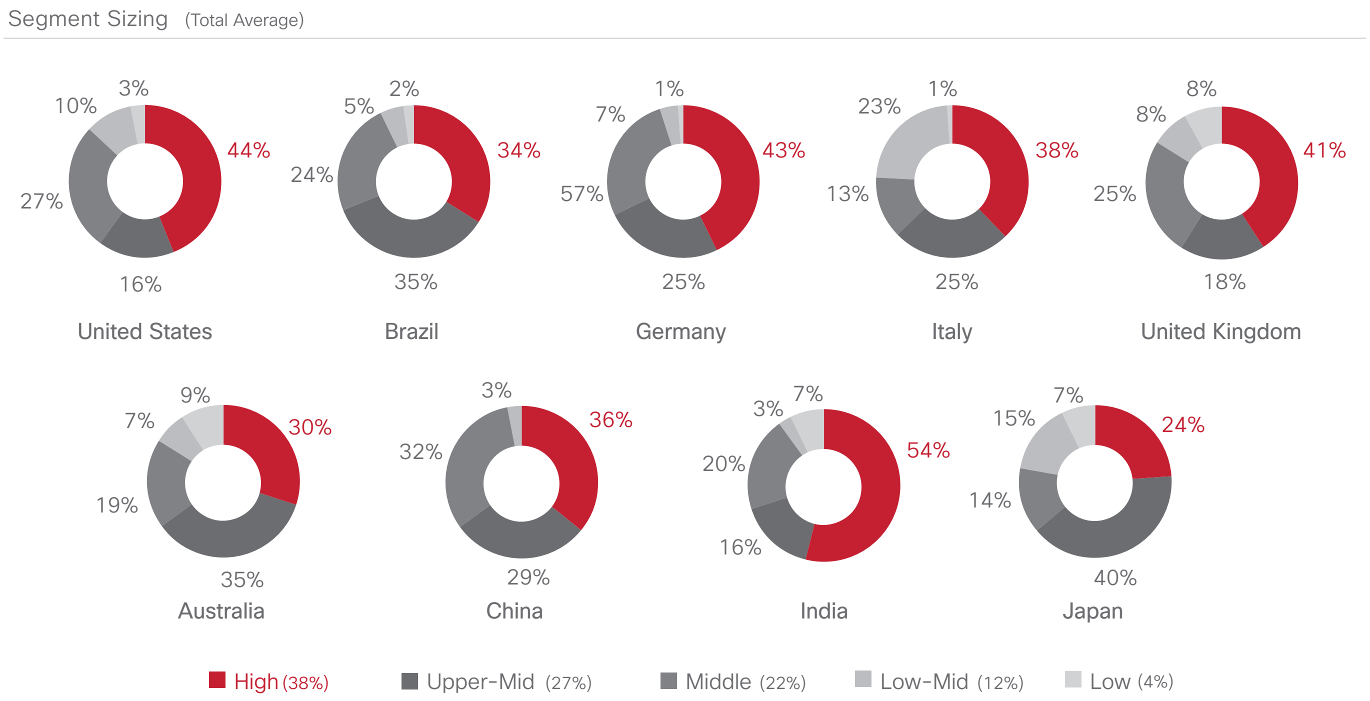
Most companies fit more sophisticated security profiles. This is true in all countries (Figure 34) and across all industries (Figure 35).

Segments reflect increasing levels of sophistication around the priority of security and how that translates into processes and procedures



Source: *Cisco Security Capabilities Benchmark Study*

Figure 34. Sophistication of Security Processes by Country

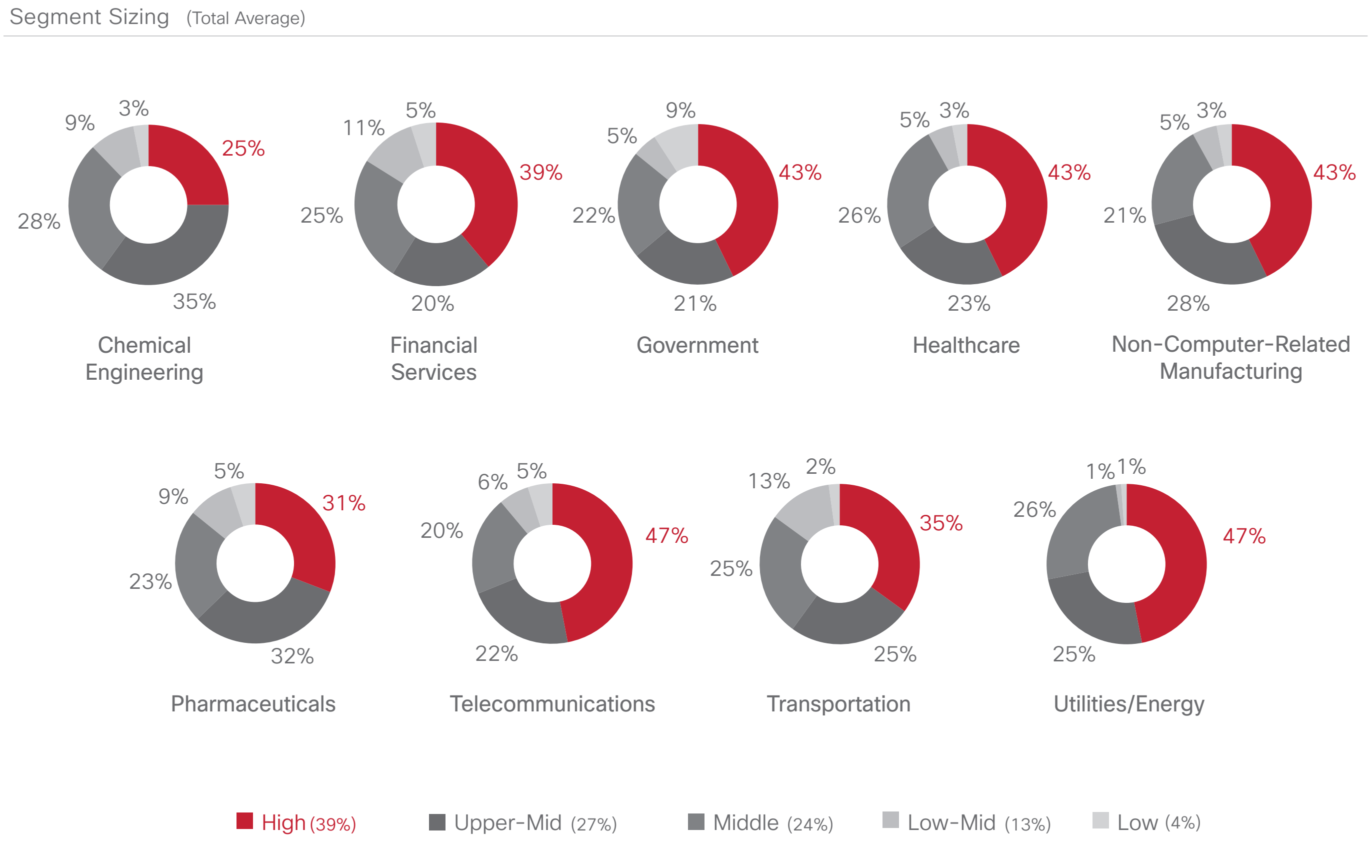


Source: *Cisco Security Capabilities Benchmark Study*

Share the report

Figure 35. Sophistication of Security Processes by Industry

Nearly half of telecommunications and utilities/energy organizations are classified into the highly sophisticated security segment.



Source: *Cisco Security Capabilities Benchmark Study*

Midmarket Organizations Appear Well Positioned for Security Readiness

Very large organizations are expected to successfully manage security because they have access to the most resources: budget for buying the latest technology, and skilled staff to manage it. Larger midsize enterprises (defined for the purposes of the study as having 500 to 999 employees) might be assumed to lag behind their larger counterparts (1000 or more employees) in terms of their readiness to respond to security incidents. However, according to the *Cisco Security Capabilities Benchmark Study,* larger midmarket enterprises appear to not only mirror enterprises in security readiness in many areas, but often rate even higher than large organizations, perhaps due to increased organization flexibility and greater agility.

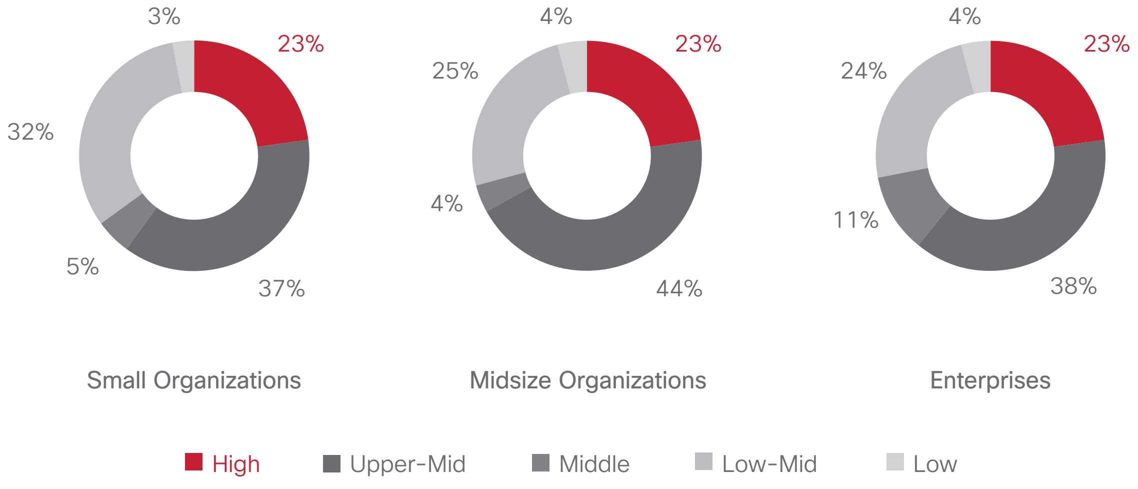
In fact, according to the study, larger midsize organizations are more likely to have highly sophisticated security postures. As illustrated in Figure 36, significantly more large midsize organizations rate in the upper midlevel and high level of sophistication than do smaller midmarket organizations (250-499 employees) and enterprise organizations (1000 or more employees).

The mostly level playing field for midmarket enterprises is promising news, since midmarket companies are the engine of the recovering economy.

Key findings from the benchmark survey on midmarket enterprises and their security readiness:

- Ninety-two percent of midsize organizations have internal incidence response teams, as opposed to 93 percent of large enterprises.
- Ninety-four percent of midsize organizations have an executive directly accountable for security, as opposed to 92 percent of larger enterprises.

Figure 36. Large Midsize Organizations' Sophistication Level in Security Posture



Segments reflect increasing levels of sophistication around the priority of security within the organization and how that translates into processes and procedures.

Significantly more midsize organizations rate in the upper-mid and high levels than do small organizations and enterprises.

At least 60 percent fit more security-sophisticated profiles.

Source: *Cisco Security Capabilities Benchmark Study*

Share the report

3. Geopolitical and Industry Trends

Cisco security, geopolitical, and policy experts identify current and emerging geopolitical trends that organizations, particularly multinational companies, should monitor. These same experts also examine recent and potential developments around the world related to the issues of data sovereignty, data localization, encryption, and data compatibility.

Cybercrime Thriving in Areas of Weak Governance

While CISOs and other security leaders may not always think to pay close attention to geopolitical dynamics, they should, especially if they work for a multinational organization. What happens in the geopolitical landscape can have a direct impact on global supply chains, and how the business manages customer and employee data in different countries; it also can create more legal and regulatory costs, risk of trade secret theft, and physical and reputational risks.

Cybercrime is flourishing around the world, especially in areas of weak governance. Eastern Europe, which has long been a hotbed of organized crime, is one example. In areas of weak governance, it is not unusual to find evidence of strong ties between government intelligence services and organized groups involved in cybercrime.

According to U.S. authorities, some recent high-profile attacks that targeted assets in the United States likely originated from such areas. Some of the attacks appeared not to be profit-oriented, but politically motivated campaigns or attempts to gather intelligence or infiltrate infrastructure.[7] This could be an indication that the campaigns were state-sponsored and/or orchestrated by sophisticated cybercrime organizations.

More governments are making a concerted effort to implement increased cyber-governance through legislation and regulation. China, for example, made "rule of law" the theme for the fourth plenum of the 18th Communist Party of China (CCP) Congress.[8] Beijing has committed to rooting out corruption and enforcing laws in business and within government. This effort may strengthen law enforcement and international efforts to track down cybercriminals and make it harder for them to hide.

Transnational Terrorist Groups Leveraging the Internet

The emergence of transnational terrorist groups, such as the so-called Islamic State (also known as ISIS or ISIL), is another geopolitical trend to watch. While groups like ISIS do not appear to be engaged in any significant cybercrime activity, they do rely heavily on the Internet—namely, social media—to recruit members. For now, it appears that leading transnational terrorist groups are making enough money through traditional fundraising activities such as extortion, human trafficking, and oil. But as these organizations grow, they could turn to cybercrime as a way to fund their efforts around the world. There is also the potential that budding terrorist organizations that do not have access to the same resources as more established groups may explore cybercrime as a fast path to growth.

See the Cisco blog post "Cupcakes and Cyberespionage," to read about a suggested new approach for defending against cyberespionage.

The Conundrum of Data Sovereignty, Data Localization, and Encryption

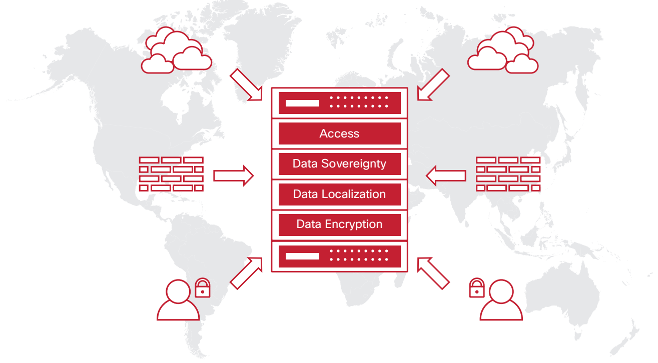
Edward Snowden's allegations about U.S. government surveillance overreach, data sovereignty (the concept that data is subject to the jurisdiction of the country where it is located and not that of foreign governments or courts that may be seeking unilateral access to it), and data localization (a government mandate that data be stored in a certain place) have become hot-button issues.

Some countries are beginning to seek the ability to localize their data as a way to prevent foreign governments from gaining access to their citizens' data. They are drafting requirements that data remain inside of their country, or be routed in certain ways, and that companies use domestically manufactured equipment.

Brazil, as an example, recently implemented a new law that "contains privacy requirements that broadly restrict [covered] companies from the sharing of users' personal information, their communications, and certain online logging data."[9] Russia, meanwhile, recently amended its data protection and information legislation to require all data operators processing personal data of Russian citizens, including Internet data, to keep copies of such data on servers and databases within Russia; the law is slated to go into effect in 2015.[10]

A potential negative consequence of countries mandating data localization—creating legislation that is not interoperable—is that multinational companies could be subjected to conflicting legal requirements. An obligation to comply with the demands of one nation to produce, retain, or destroy data could violate the laws of another country.

Figure 37. The Conundrum of Balancing Data Sovereignty, Localization, and Encryption



Aside from potentially causing conflicting legal obligations, data localization requirements also have the potential to restrict the flow of data across borders. This can create confusion, as well as significant challenges in administering networks. There is a supply chain aspect here as well: More global supply chain operators are adopting cloud-based technology to connect all of their partners around the world. Data localization could hinder, or prevent data exchange in those business networks, and potentially hinder cross-border activities to police cybercrime activity.

Additionally, as some countries opt to use only homegrown technologies, or place significant restrictions on who can handle their citizens' data, there is the potential that they will cut themselves off from the global talent pool and possibly risk a loss of innovation that comes from cross-pollination of new ideas.

Some leading technology companies in the United States are hoping that use of end-to-end encryption will be a way to satisfy their customers' concerns that their data be protected as it traverses the borderless Internet. The U.S. government has raised concerns, however, that such encryption will prevent its ability to protect citizens. The new director of the GCHQ, Britain's premier signals intelligence organization, similar to the U.S. National Security Agency, even suggested that U.S. social media technology giants are aiding the efforts of terrorists by enabling them to send encrypted communications around the world.[11]

Despite these criticisms, technology companies are likely to continue to pursue the development and adoption of technological measures aimed at restoring customer trust until governments have adopted policies that more effectively reflect the importance of enabling free speech and secure commerce while they protect against threats to public safety and national security.

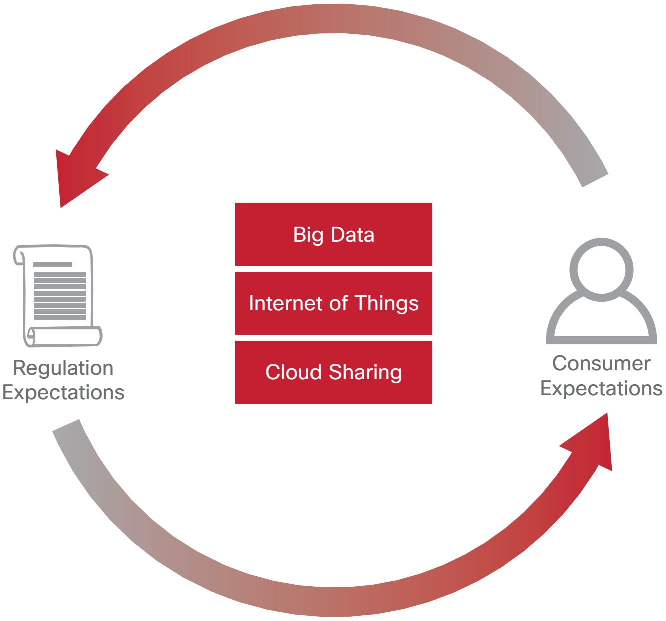
Trust in technology products, and in the companies that develop them, will go a long way toward countries and their governments and citizens having confidence that they, and their data, are protected. As Mark Chandler, Cisco senior vice president, general counsel, and secretary, noted in a Cisco blog post earlier this year, "A serious effort to address these issues can build confidence, and most importantly, result in the promise of the next generation of the Internet being met, a world in which the connection of people and devices drives greater freedom, prosperity, and opportunity for all the world's citizens."[12]

Data Privacy Compatibility

A person's or organization's attitudes about data privacy can vary greatly depending on where in the world they live and work. These varied viewpoints affect how governments regulate data privacy, and how enterprises do business when these regulations are at odds with each other. The ***Data Protection Heat Index Survey Report***, sponsored by Cisco and prepared by the Cloud Security Alliance, details some of the challenges faced by enterprises working with data outside of their own countries, or data that belongs to individuals outside of the country in which the business operates.

The conversation around data privacy compatibility—that is, creating consistent global approaches to data privacy—has become more urgent due to the growth of cloud services. For example, if a company based in the United States purchases cloud storage from a company in India, and used that cloud to store data for customers residing in Germany, which region or country's privacy laws apply?

Figure 38. Meeting Diverse Regulatory and Consumer Expectations



Other drivers of data privacy compatibility are the Internet of Things (IoT) and big data. As enterprises consider new ways to connect devices to each other, and use massive datasets to make business decisions, they need structure and rules for how this data may be handled on a global scale.

Various efforts are under way aimed at harmonizing data privacy requirements across a region or group of countries. For example, European Union legislation is currently being shaped that will update the existing data protection framework—the *General Data Protection Regulation,* calling for a harmonization of data protection regulations. Efforts to achieve consensus around data privacy and data sovereignty laws are intensifying. Greater harmonization would be welcome, but it is also important that the final text is outcome-oriented, interoperates with other regions, and is appropriate for the new technology realities. The Asia-Pacific region has developed the Cross-Border Privacy Enforcement Arrangement from the Asia-Pacific Economic Cooperation (APEC), which facilitates data sharing in local economies. More work must be done by governments to meet the larger goal of creating compatible regimes for data privacy and security anchored in globally recognized standards that promote an open Internet with free flows of data across both national and regional borders.

As countries and regions clarify their data privacy approaches, enterprises will be better able to apply consistent privacy practices globally, and implement more effective "privacy by design" frameworks, in which privacy capabilities are built into products and services right from the start. Clear and consistent privacy regulatory frameworks would help companies meet and exceed privacy requirements, no matter where their offerings are being deployed, thereby encouraging innovative product development and use of data.

Data Privacy: A Shared Understanding

The data protection survey asked global privacy experts in North America, the European Union, and the Asia-Pacific region about regulation of data in their region, governmental practices, user content, and security standards. Responses showed a high level of consistency in respondents' understanding of the meaning of data privacy, and in the value of global privacy standards.

- ▶ **Data residency and sovereignty:** Respondents identified personal data and personally identifiable information (PII) as the data that is required to remain resident in most countries.
- ▶ **Lawful interception:** Respondents showed a universal interpretation of when and how data may be intercepted—for example, when it's needed for a criminal investigation.
- ▶ **User consent:** Seventy-three percent of respondents agreed that there should be a consumer privacy bill of rights that is global in nature as opposed to regional. Sixty-five percent said that the United Nations should play an active role in the creation of such a bill.
- ▶ **Privacy principles:** Respondents were asked if privacy principles from the Organisation for Economic Cooperation and Development would facilitate data harmonization, or would instead create greater tension. The data privacy experts surveyed were largely in favor of the adoption of these principles.

In sum, the data privacy survey seems to show that many experts agree on basic privacy principles that, if adopted and standardized globally, can be an enabler of business, not an obstacle. The results also indicate that data privacy experts share an interest in "baking in" privacy principles for new technology solutions, instead of trying to retrofit these solutions to accommodate privacy requirements. However, current privacy regulatory frameworks are relatively nascent and evolving rapidly.

Should a greater level of harmonization advance, companies and individuals will benefit. But to the extent that industry continues to see discordant privacy frameworks globally, companies will need to think through privacy and data protection issues carefully, and proactively adapt their offerings and processes to meet diverse customer and regulatory expectations.

To learn more about data protection issues, see the Cisco Security blog post, "Data Protection in the Balance–EU Citizen Protection and Innovation."

4. Changing the View Toward Cybersecurity—From Users to the Corporate Boardroom

Cisco security experts suggest that it is time for enterprises to start looking differently at how they approach cybersecurity so they can truly make their organizations more secure. Strategies include considering new approaches to help align people, processes, and technology, making security a topic at the corporate boardroom level, and adopting more sophisticated security controls that can reduce the endpoint and attack surface—and harden the network after an attack.

Secure Access: Understanding Who Is on Your Network, When, and How

CISOs and other security professionals are faced with complex challenges regarding access to network information and services. Thanks to the trends toward mobility and bring-your-own-device (BYOD) policies, they must ensure that employees can gain access to enterprise resources, no matter where they happen to be, and no matter how they join the network.

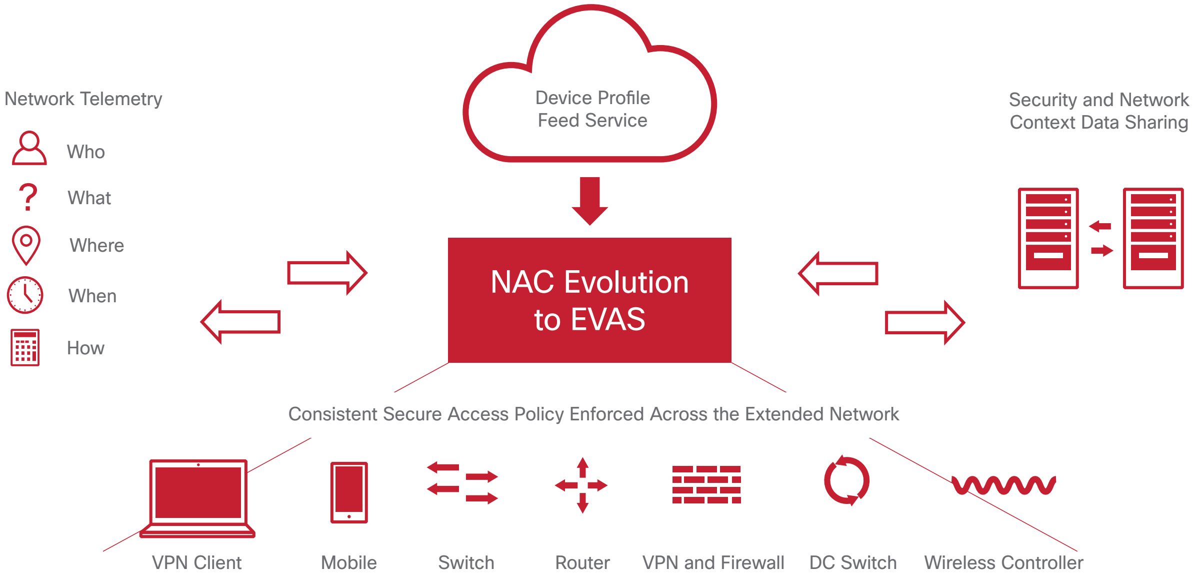
Security professionals also need to protect the network from unapproved users or criminal attacks, and they must do so in a way that doesn't impede access by legitimate users. For example, virtual private networks (VPNs) used to be the standard solution for providing network access control. However, some VPNs call for complicated login procedures by users as well as special software, limiting when and how people join the network. In addition, many VPNs don't help IT departments identify who is gaining access and from where, nor can VPNs identify the devices in use. VPNs are evolving to provide more visibility, while producing a more transparent user experience in order to provide better endpoint security.

Network access controls (NACs) are evolving away from basic security protection to more sophisticated endpoint visibility, access, and security (EVAS) controls. Unlike older NAC technologies, EVAS use more granular information to enforce access policies, such as data about user role, location, business process considerations, and risk management. EVAS controls also help grant access beyond computers, allowing network administrators to provide access through mobile and IoT devices.

EVAS help enable a network-as-a-sensor approach to security enforcement, granting or halting access throughout the extended network, whether from a remote device (VPN), prior to connecting to network services, or even within the network itself across sensitive resource pools. EVAS can also help organizations reduce the endpoint and network attack surface, limit the scale and scope of an attack, remediate problem resolution processes, and even harden the network after an attack has occurred.

For more information about EVAS solutions and how they can help organizations improve security, see the Cisco Security blog post, "New White Paper from Enterprise Strategy Group on the Evolution of and Need for Secure Network Access."

Figure 39. The Evolution of Network Access Controls (NACs) to Endpoint Visibility, Access, and Security (EVAS) Controls


Network Telemetry
Who
What
Where
When
How
Device Profile Feed Service
NAC Evolution to EVAS
Security and Network Context Data Sharing
Consistent Secure Access Policy Enforced Across the Extended Network
VPN Client
Mobile
Switch
Router
VPN and Firewall
DC Switch
Wireless Controller

Before an attack, EVAS can:

- **Identify risky assets.** Monitor all assets connected to the network at any time, identifying non-compliant users, devices, and applications, and correlate this information with third-party vulnerability assessment tools.
- **Improve risk mitigation.** Gather actionable intelligence that can be shared with other security and network applications to improve workflows, streamline operations, and prioritize remediation activity.
- **Enforce granular network access policies.** Provide contextual information for granular policy enforcement, and limit access to sensitive content, assets, or network segments.

During an attack, EVAS can:

- **Integrate with advanced network-based threat defense systems.** Share knowledge when malicious activity is detected for the purpose of correlating attack data endpoint connections, configurations, and behavior patterns over time.
- **Block "kill chain" tactics from compromised systems.** Limit lateral attack movement by stopping compromised systems from reaching out to policy-controlled, non-authorized network assets to steal credentials, escalate privileges, and exfiltrate valuable data.
- **Limit the scope of an attack.** Restrict and thereby quarantine systems that exhibit anomalous behavior.

After an attack is detected, EVAS can:

- **Assess endpoint profiles for vulnerabilities.** Share information from the EVAS database with vulnerability analysis tools, which can help IT operations prioritize a fix.
- **Remediate compromised systems.** When integrated with security information and event management (SIEM) systems, and endpoint security systems, EVAS can automate fixes and monitor progress.
- **Fine-tune access policies and security controls.** Work with networking and security equipment to segment application traffic or add new firewall rules or IPS signatures.

Unlike overly complex network access controls of the past, EVAS solutions are business enablers. As organizations embrace BYOD policies, cloud computing, and mobility initiatives, gaining visibility, improving context into connected users and devices, and effectively enforcing security policies become more imperative. Cisco security experts predict that CISOs will increasingly turn to EVAS solutions to manage the complex web of connections among users, devices, networks, and cloud services.

Share the report

The Future of Cybersecurity Hinges on Boardroom Engagement Today

According to the *Cisco Security Capabilities Benchmark Study*, 91 percent of organizations have an executive with direct responsibility for security. But for modern businesses, security leadership needs to ascend even higher in the organization: to the boardroom.

Recent, massive data breaches involving well-known companies, more legislation and regulation related to data security, geopolitical dynamics, and shareholder expectations are all factors making cybersecurity an agenda item in the boardroom. A report by the Information Systems Audit and Control Association (ISACA) revealed that 55 percent of corporate directors now have to personally understand and manage cybersecurity as a risk area.[13]

This is a positive development, but one that Cisco security leaders believe is long overdue. In the modern economy, every company runs on IT. That makes security the business of every person in the organization, from the chief executive to the newest hire, and not just personnel with "security" in their title or job description. Everyone should be accountable, and learn how not to be a victim.

Cisco security leaders assert that a core component of the future of cybersecurity will be greater engagement by the board. Corporate boards of directors across industries need to know what the cybersecurity risks to the business are and their potential impact. To truly understand the scope of cybersecurity issues that affect the organization, some boards may need to add members with technology and cybersecurity expertise.

Boards also need to start asking tough questions about security controls: *What controls do we have in place? How well have they been tested? Do we have a reporting process? How quickly can we detect and remediate the inevitable compromise?* And perhaps, the most important question: *What else should we know?* CIOs need to be prepared to answer those questions from the board, in terms that are meaningful to board members, and also outline business implications.

In a recent interview with FORTUNE magazine,[14] Cisco Chief Security and Trust Officer John Stewart said that the board asking these types of questions will help spark "an interesting set of downstream effects" that ultimately will lead to the security industry maturing. From there, he said, the next vital step—the hope—will be that manufacturers finally recognize that they must build security into their products.

Stewart predicts that as the Internet of Things (IoT) evolves, and there are more "people-less devices on the Internet than people-with devices" there will be inevitable "accidents" of potentially great magnitude. Designing security into products will help to avoid many of these issues, or at least, lessen their impact.

Therefore, the boards of technology manufacturers should ask their security leaders: *Are we building security into our products? And if not, how soon can we start?*

View the video blog by Cisco Chief Security and Trust Officer John Stewart on the importance of cybersecurity transparency and accountability to the board: http://blogs.cisco.com/security/ensuring-security-and-trust-stewardship-and-accountability.

Cisco Security Manifesto: Basic Principles for Achieving Real-World Security

Today's CISOs need to answer hard questions: *How do I make my security team the first point of contact for the business when potential security issues arise? How can I ensure my team has the tools and visibility to determine what security issues are most relevant, and require action? And how do I keep users—the key to business success—safe, and not just when they are working on-site?*

Cisco security experts suggest that CISOs can address these questions by implementing and following a set of security principles known as the Cisco Security Manifesto.

This inaugural security manifesto can help security teams, and the users in their organizations, to better understand and respond to the cybersecurity challenges of today's world. These principles can serve as a baseline for organizations as they strive to become more dynamic in their approach to security, and more adaptive and innovative than adversaries:

1. **Security must be considered a growth engine for the business.** Security should never be a roadblock or hassle that undermines user productivity and stands in the way of business innovation. Yet security teams impose technological solutions that do exactly that. A primary reason: They are not invited in time, or at all, to discussions about business projects that require the deployment of new technology. However, security professionals are also guilty of waiting for an invitation they may never receive. They instead must take proactive steps to ensure they are involved in technology conversations, and understand how security processes can enable the organization's agility and success, while also protecting its data, assets, and image.

2. **Security must work with existing architecture, and be usable.** Security teams should not have to build an architecture to accommodate new technology solutions that are meant to improve security. Architectures, by nature, are constraining. Organizations should not have to change the way they do business to accommodate new security technologies, or be prevented from making changes in how they operate because of the technologies they already have in place. The end result of "architecture overload" is that users will circumvent security architecture, leaving the organization less secure. In addition, if a security technology is too difficult for users to understand, and must be maintained by hard-to-find, specialized security talent, it is not useful to the organization.

3. **Security must be transparent and informative.** Users should be presented with information that helps them understand why security is stopping them from taking a particular action. They also need to know how they can do what they want to do safely, instead of bypassing security in the name of doing their jobs. As an example, when a user attempts to access a web page and is met with the message, "Access to this site has been denied by your administrator," there is no context as to why they can't access the page. But if the message said, "Access to this site has been denied because it has served malware in the last 48 hours," the user would be better informed and understand the potential risk not only to the organization, but to them, as an individual user. Security technologies also should help users to achieve their goals safely through clear recommendations or by directing them to appropriate resources for timely assistance.

4. **Security must enable visibility and appropriate action.** Security solutions with open security architecture enable security teams to determine whether those solutions are truly effective. Security professionals also need tools for automating visibility into the network so they not only can see traffic, but also the assets that make up the network. By understanding how security technologies operate, and what is normal (and not normal) in the IT environment, security teams can reduce their administrative workload while becoming more dynamic and accurate in identifying and responding to threats and adapting defenses. In taking this approach, security teams can take full advantage of more relevant and targeted controls to aid in resolution.

5. **Security must be viewed as a "people problem."** A technology-centric approach to security does not improve security; in fact, it exacerbates it. Technologies are merely tools that can enhance the ability of people to secure their environment. Security teams need to educate users about safe habits that they should apply no matter where they are using technology—at the office, at home, on the road—so they can make good decisions and feel empowered to seek timely assistance when they think something is wrong. Improved dialogue between security professionals and users will also help users see that technology alone cannot assure security. People, processes, and technology, together, must form the defense against today's threats. Commitment and vigilance by all users in the organization, from the top down, empower security success.

The Cisco Security Manifesto is a call for a change. In the real world, security technology, policies, and best practices should raise the average level of security for everyone in the organization, and help the business make more informed risk decisions—down to each individual user. And with strong principles to guide them, users can gain a clear understanding of why they are prevented from taking certain actions, and what the impact likely would be if they decide to bypass security.

The Cisco Security Manifesto, or one that echoes its core principles, can help both users and security practitioners to see the "big picture" on security: While many threats can be avoided, compromise is inevitable—but remediation can be swift. The goal is to reduce the time to resolution when a compromise is eventually successful, and not focus solely on trying to prevent these events.

About Cisco

Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced threat protection portfolios of solutions across the broadest set of attack vectors. Cisco's threat-centric and operationalized approach to security reduces complexity and fragmentation while providing superior visibility, consistent control, and advanced threat protection before, during, and after an attack.

Threat researchers from the Collective Security Intelligence (CSI) ecosystem bring together, under a single umbrella, the industry's leading threat intelligence, using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open source community at Cisco. This amounts to a daily ingest of billions of web requests and millions of emails, malware samples, and network intrusions.

Our sophisticated infrastructure and systems consume this telemetry, enabling machine-learning systems and researchers to track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, email, and from the cloud to identify root causes and scope outbreaks. The resulting intelligence is translated into real-time protections for our products and services offerings that are immediately delivered globally to Cisco customers.

The CSI ecosystem is comprised of multiple groups with distinct charters: Talos, Security & Trust Organization, Managed Threat Defense (MTD), and Security Research and Operations (SR&O).

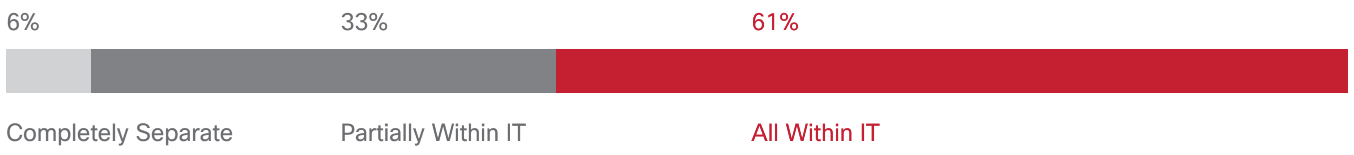
To learn more about Cisco's threat-centric approach to security, visit www.cisco.com/go/security.

Appendix

Additional Security Capabilities Benchmark Study Findings

Resources

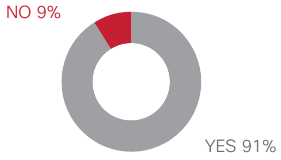
Is the security budget part of the IT budget? IT Department members; n=1720



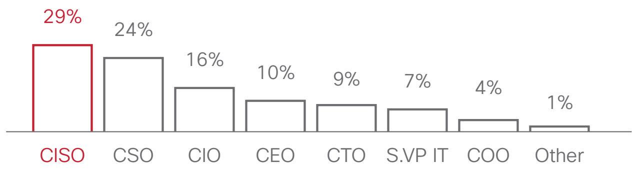
Security Policies, Procedures, and Operations

Highest ranking executive accountable for security is most often a CISO or CSO.

Is there an executive at your organization who has direct responsibility and accountability for security?
Respondents who report clarified roles and responsibilities; n=1603



Executive's Title
Respondents who report executive with security responsibility; n=1465



Healthcare is less likely than other industries to identify an executive accountable for security.

Share the report

Nearly two-thirds say that executive leadership considers security a high priority.

Executive Engagement n=1738	SecOps n=797			CISO n=941		
	Disagree/	Agree/	Strongly Agree	Disagree/	Agree/	Strongly Agree
Executive leadership at my organization considers security a high priority	8%	34%	58%	3%	30%	67%
Security roles and responsibilities are clarified within my organization's executive team	9%	39%	52%	2%	32%	64%
My organization's executive team has established clear metrics for assessing effectiveness of our security program	11%	44%	45%	4%	37%	59%

More respondents who report they have not had to manage public scrutiny of a security breach in the organization strongly agree with “executive leadership at my organization considers security a high priority.”

High proportions report security processes that encourage employee participation.

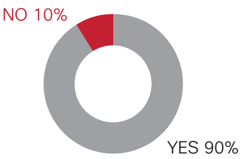
Security Processes n=1738	SecOps n=797			CISO n=941		
	Disagree/	Agree/	Strongly Agree	Disagree/	Agree/	Strongly Agree
Line-of-business managers are encouraged to contribute to security policies and procedures	12%	39%	49%	6%	40%	54%
My organization is able to detect security weaknesses before they become full-blown incidents	13%	43%	44%	4%	39%	57%
Employees at my organization are encouraged to report failures and problems with security	11%	34%	55%	4%	36%	60%
Security processes and procedures at my organization are clear and well understood	13%	39%	48%	4%	37%	59%
Security processes at my organization enable us to anticipate and mitigate potential security issues proactively	14%	40%	46%	3%	40%	47%
Security processes at my organization are measured and controlled using quantitative data	13%	40%	47%	4%	35%	61%
My organization has optimized its security processes and is now focused on process improvement	12%	42%	46%	4%	36%	60%

Security professionals from midmarket organizations tend to express higher levels of agreement with security process items than do enterprise professionals.

Nine in 10 respondents say regular security training is provided to security employees—typically delivered by the security team.

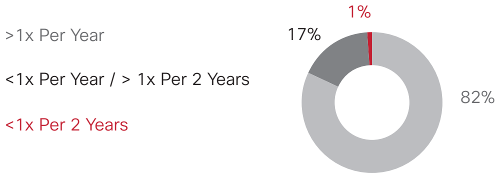
Are security awareness and/or training programs delivered to security staff on a regular basis?

Respondents dedicated to security; n=1726



How often is security training delivered?

Respondents dedicated to security; n= 1556

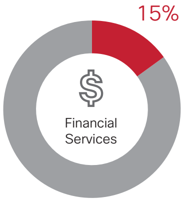


Who delivers security training?

Respondents whose security teams receive training; n=1556

Internal security team	Third-party contractors	Human resources	Other employees	Other
79%	38%	25%	10%	1%

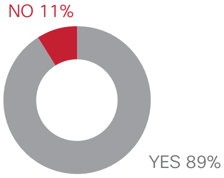
Fifteen percent of financial services professionals say security training is not offered regularly.



Staff commonly attend conferences or training; about two-thirds say they're involved in security industry associations.

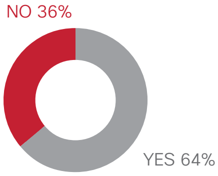
Do security staff members attend conferences and/or external training to improve and maintain their skills?

Respondents dedicated to security; n=1715



Do employees serve on security industryboards or committees?

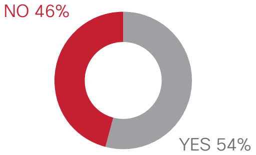
Respondents dedicated to security; n=1690



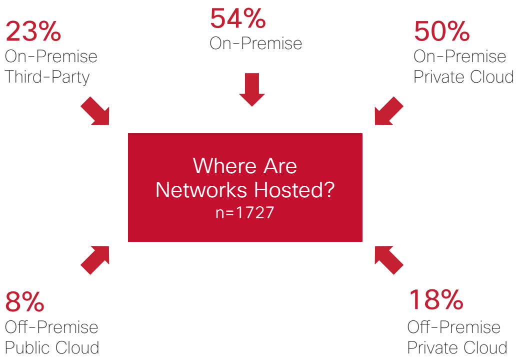
Over half of respondents say their organization has had to manage public scrutiny of a security breach.

Has your organization ever had to manage public scrutiny of a security breach?

Respondents dedicated to security; n=1701



On-premise hosting of the organization’s networks is most common; fewer than one in 10 report they are hosted in a public cloud.



Significantly more SecOps respondents say off-premise hosting (both private and public cloud) is used in their organization, compared to CISOs.

Sophistication

Segments vary predictably on many measures of security sophistication ...

	Low	Low-Mid	Middle	Upper-Mid	High
Company executives consider security a high priority	22%	38%	45%	71%	81%
... and have clear metrics for assessing security program effectiveness	17%	19%	32%	52%	79%
The company has clear, well-understood security processes/procedures	0%	22%	15%	72%	88%
... that are measured and controlled using quantitative data	0%	17%	33%	65%	76%
... and regularly reviews security practices and tools to ensure they're up to date and effective	0%	17%	33%	65%	76%
The company does an excellent job managing HR security through onboarding and good processes for transfers and departures	16%	27%	36%	52%	76%
Information assets are inventoried and clearly classified	17%	26%	40%	58%	73%
Computer facilities within my organization are well protected	17%	21%	41%	63%	80%
Security technologies are well integrated to work effectively together	17%	21%	38%	59%	78%
... the company is able to detect security weaknesses before they become full-blown incidents	0%	23%	25%	63%	70%

But not on all ...

	Low	Low-Mid	Middle	Upper-Mid	High
There is an executive with direct responsibility and accountability for security	85%	91%	88%	93%	93%
The company has a written, formal organization-wide security strategy that's reviewed regularly	59%	47%	58%	65%	60%
The company follows a standardized information security policy practice such as ISO 27001	47%	44%	50%	59%	54%

Endnotes

1. *Cisco 2014 Midyear Security Report:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.

2. For more on CMS vulnerabilities, see "Wordpress Vulnerabilities: Who Is Minding the Store?", *Cisco 2014 Midyear Security Report:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027 .

3. "Goon/Infinity/RIG Exploit Kit Activity," Cisco IntelliShield: Security Activity Bulletin, July 2014: http://tools.cisco.com/security/center/mviewAlert.x?alertId=34999.

4. *Cisco 2014 Midyear Security Report:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.

5. "Cisco Event Response: POODLE Vulnerability," October 15, 2014: http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Poodle_10152014.html.

6. "OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations," Cisco Security Blog, April 9, 2014: http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations

7. "JP Morgan and Other Banks Struck by Hackers," by Nicole Perlroth, *The New York Times,* August 27, 2014: http://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html?_r=0; "'Trojan Horse' Bug Lurking in Vital U.S. Computers Since 2011," by Jack Cloherty and Pierre Thomas, ABC News, November 6, 2014: http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476.

8. "4 Things We Learned from China's 4th Plenum," by Shannon Tiezzi, *The Diplomat,* October 23, 2014: http://thediplomat.com/2014/10/4-things-we-learned-from-chinas-4th-plenum/.

9. "Brazil's New Internet Law Could Broadly Impact Online Privacy and Data Handling Practices," *Chronicle of Data Protection,* May 16, 2014: http://www.hldataprotection.com/2014/05/articles/international-eu-privacy/marco-civil-da-internet-brazils-new-internet-law-could-broadly-impact-online-companies-privacy-and-data-handling-practices/.

10. "Russian data localization law may now come into force one year ahead of schedule, in September 2015," by Hogan Lovells, Natalia Gulyaeva, Maria Sedykh, and Bret S. Cohen, Lexology.com, December 18, 2014: http://www.lexology.com/library/detail.aspx?g=849ca1a9-2aa2-42a7-902f-32e140af9d1e.

11. "GCHQ Chief Accuses U.S. Tech Giants of Becoming Terrorists' 'Networks of Choice,'" by Ben Quinn, James Ball, and Dominic Rushe, *The Guardian,* November 3, 2014: http://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan.

12. "Internet Security Necessary for Global Technology Economy," by Mark Chandler, Cisco Blog, May 13, 2014: http://blogs.cisco.com/news/internet-security-necessary-for-global-technology-economy.

13. "Cybersecurity: What the Board of Directors Needs to Ask," ISACA and The Institute of Internal Auditors Research Foundation, August 2014: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx.

14. "It's Time for Corporate Boards to Tackle Cybersecurity. Here's Why," by Andrew Nusca, FORTUNE magazine, April 25, 2014: http://fortune.com/2014/04/25/its-time-for-corporate-boards-to-tackle-cybersecurity-heres-why/.

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.