

WSTR

WEBSITE SECURITY THREAT REPORT | 2015

PART 2

CONTENTS

Targeted Attacks	3
Data Breaches	20
Recommendations	30
About Symantec	34



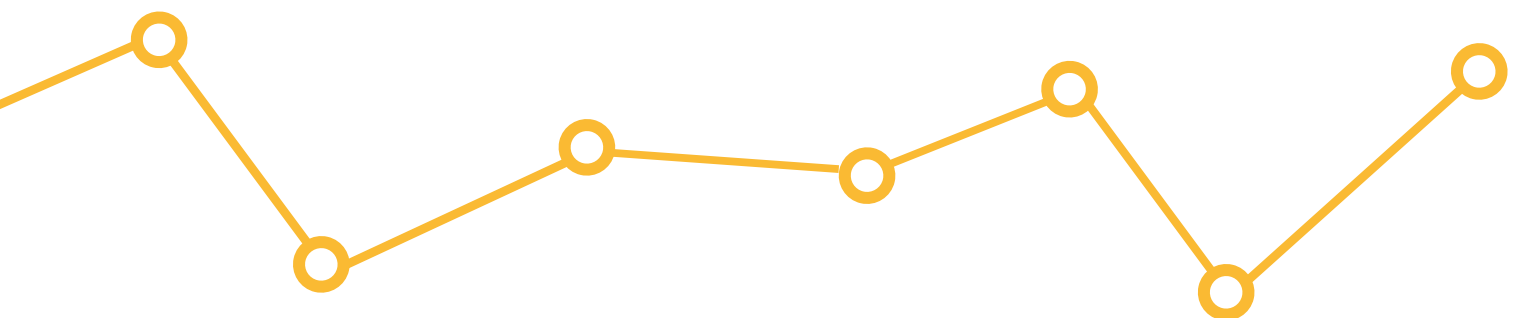
TARGETED ATTACKS

The logo for WSTR is centered within a dark grey rectangular box with a white border. The letters 'W', 'S', and 'T' are rendered in a white, outlined, sans-serif font. The letter 'R' is rendered in a solid, bold, orange sans-serif font. A white line with circular nodes at its ends passes behind the box, extending from the left edge to the right edge of the page.

WSTR

AT A GLANCE

1	More state-sponsored cyberespionage came to light in 2014.
2	Attackers are using increasingly well-crafted malware that display sophisticated software engineering and professionalism.
3	Campaigns such as Dragonfly, Waterbug, and Turla infiltrated industrial systems, embassies, and other sensitive targets.
4	The number of spear-phishing campaigns increased by 8 percent in 2014, while the number of daily attacks decreased as attackers become more patient, lying in wait, and crafting more subtle attacks boosted by longer-term reconnaissance.



INTRODUCTION

In 2014, Symantec analyzed several cyberespionage attacks and gathered data on the tactics used to infiltrate thousands of sensitive and well-defended organizations around the world. This research shows a worrying increase in sophistication.

Imagine you're the CISO for an Eastern European diplomatic corps. In 2014, you suspect that computers in your embassies across Europe have been infected with a backdoor Trojan. You call in a security firm to investigate, and they confirm your worst suspicions. Upon investigation you find that a very carefully targeted spear-phishing campaign sent emails to members of staff with a stealthy Trojan payload that infected the computers. The use of zero-day exploits, carefully-crafted emails, and cunning watering-hole website attacks meant that the attacks evaded detection long enough to compromise more than 4,500 computers in over 100 countries¹.

It's a worrying scenario, but not a hypothetical one. This is a description of the Waterbug attack.

It is similar to other targeted attacks such as Turla and Regin, and due to the targets chosen and the sophistication of the attacks methods, Symantec believes that a state-sponsored group is behind Waterbug².

In view of the growing sophistication of these attacks, good IT security is essential, and broad cybersecurity practices should be the norm. Well-funded state actors are not the only threat. Patriotic hackers, hacktivists, criminal extortionists, data thieves, and other attackers use similar techniques, but with fewer resources and perhaps less sophistication.

Email-based attacks continue much as before. Web-based attacks are growing increasingly sophisticated. Espionage attacks use more exploit kits, bundling together exploits rather than using just one attack. Exploit kits have been used in e-crime for many years, but now many cyberespionage attackers are using them too.

¹ http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf

² Ibid

CYBERESPIONAGE

In 2014, Symantec security experts spent nearly eight months dissecting one of the most sophisticated pieces of cyberespionage they had ever seen. Known as Regin, it gives its owners powerful tools that were used to spy on governments, infrastructure operators, businesses, researchers, and private individuals. Attacks on telecoms companies appear to be designed to gain access to calls being routed through their infrastructure³.

Regin is complex, with five stealth stages of installation. It also has a modular design that allows for different capabilities to be added and removed from the malware. Both multi-stage loading and modularity have been seen before, but Regin displays a high level of engineering capability and professional development. For example, it has dozens of modules with capabilities such as remote access, screenshot capture, password theft, network traffic monitoring, and deleted file recovery⁴.

It took months—if not years—to develop Regin, implying a significant investment of resources. It is highly suited to persistent long-term surveillance operations, and its level of sophistication implies that a nation state created it.

Symantec saw a similar level of commitment in another cyberespionage campaign known as Turla⁵. The attackers used spear phishing and watering-hole attacks to target the governments and embassies of former Eastern Bloc countries. Once installed, it gave attackers remote access to infected computers, allowing them to copy files, delete files, and connect to servers, among other things. Because of the targets chosen and the sophistication of the malware, Symantec believes that a state-sponsored group was behind these attacks too⁶.

More recently, a highly resourced attack group dubbed the “Equation Group” was exposed⁷, revealing that espionage attacks in previous years, including 2014, had probably employed highly specialized tactics. Moreover, as espionage attack groups continue to improve their techniques, they can also take advantage of the black market in exploits, zero-day attacks, and custom code. The exposé of the Equation Group further highlights the professionalism behind the development of these specialized attacks, as espionage attack groups benefit from the same traditional software development practices as legitimate software companies.

³ <http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance>

⁴ <http://www.symantec.com/en/uk/outbreak/?id=regin>

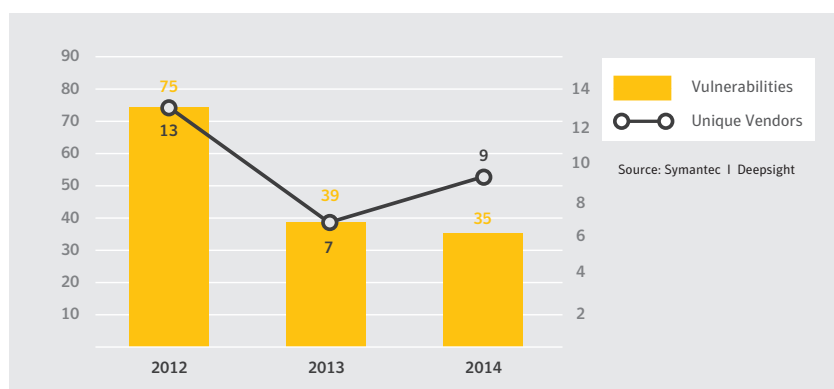
^{5,6} <http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats>

⁷ <http://www.symantec.com/connect/blogs/equation-advanced-cyberespionage-group-has-all-tricks-book-and-more>

INDUSTRIAL CYBERSECURITY

As more devices are being connected to the Internet, new avenues of attack and, potentially, sabotage open up. This is especially true for industrial devices known as Industrial Control Systems (ICS), commonly used in areas of industrial production and utility services throughout the world. Many of these devices are Internet-enabled, allowing for easier monitoring and control of the devices.

VULNERABILITIES DISCLOSED IN ICS INCLUDING SCADA SYSTEMS, 2012 – 2014



The chart shows the number of disclosed vulnerabilities that were associated with ICS and SCADA (Supervisory Control And Data Acquisition) systems, including the number of vendors involved each year.

Symantec saw many attacks against industrial control systems in 2014. For example, the Dragonfly cyberespionage campaign attacked a range of targets, including energy grid operators, electricity generators, petroleum pipeline operators, and industrial equipment manufacturers⁸. The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland.

While, by attacking industrial control systems, it follows in the footsteps of Stuxnet, which targeted the Iranian nuclear program, Dragonfly appears to have less destructive goals. Initially, it appears focused on espionage and persistent access rather than the ultimate goal of sabotage. However, it gives the well-resourced group who created it insight into important industrial systems and—hypothetically—the ability to deliver a more destructive attack if required.

Using custom-written malware and malware bought ‘off the shelf’ from Russian-language forums, it was spread using a combination of email-based spear phishing, and web-based watering-hole attacks that targeted principle victims through smaller, less well-protected companies in their supply chain.

It can be difficult for companies to protect legacy systems when they can’t afford any downtime for patching, or when they use proprietary or poorly-protected technology. For example, OLE for Process Control⁹ (OPC) is a widely used protocol in industrial automation systems. It is a well-documented open standard but there is little provision for encryption, authentication, or other security measures, making it vulnerable to rogue software. One of the goals of Dragonfly was to collect information about OPC systems in target companies.

By specifically exploiting the ICS vendors’ software update servers, the Dragonfly attacks introduced a new dimension to the watering-hole attack method. Watering-hole-based attacks exploit vulnerabilities in third-party web sites that the real target of the attack will visit, through which the attacker may inject malware into the targeted organization. With Dragonfly, the attackers compromised the supply chain by exploiting the software update servers for the ICS software employed by its victims, marking a new milestone in new watering-hole-style attacks.

⁸ <http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat>

⁹ http://en.wikipedia.org/wiki/OLE_for_Process_Control

RECONNAISSANCE ATTACKS

Besides attacks using spear-phishing campaigns and watering-holes—which require the human element of social engineering to succeed—hackers continue to attack targeted organizations from other angles in order to gain a foothold in their network. They can do this by scanning the perimeter of the network, looking for holes in their defenses and exploiting them.

Now more than ever, reconnaissance plays a big part in the process of an attacker gaining access to a targeted organization's network. This is generally the first step in the hacking process: gaining information about the systems and looking for any weaknesses that can be exploited.

The popularity of reconnaissance is clear when looking at the top zero-day exploits in 2014. Far and away, the most commonly used zero-day vulnerability was CVE-2013-7331. This wasn't your run-of-the-mill, exploit-and-gain-access-to-a-vulnerable-system sort of exploit either. All it allows is for the attacker to gather intel on the targeted network. However, it is quite useful for planning further attacks. Armed with information such as the targeted, internal network's hostnames, IP addresses, and various internal path names, an attacker could easily figure out his or her next plan of attack.

This zero-day was also left unpatched for a significant period of time. Not only was the CVE for this vulnerability allocated in 2013, only to be disclosed in February 2014, but the patch to mitigate this vulnerability wasn't released until September 2014. This left a huge window of 204 days between public disclosure and patch for use by attackers.

The best explanation for this extended period of exposure is perhaps the perceived severity of the threat. Since this particular exploit did not allow an attacker to directly take control of a vulnerable computer, it was perhaps not considered as important to address as other vulnerabilities. Attackers clearly noticed this, and were able to take advantage of the vulnerability and the information it gave them about targeted networks, indirectly helping them in their malicious goals.

This is a portion of the threat landscape that may be deserving of more attention across the security industry. While a vulnerability that simply returns information about the network, computer, or device may not be considered as severe as one that allows privilege escalation, it can nevertheless be just as dangerous if it points attackers toward vulnerable systems they would not have discovered without it.

WATERING-HOLE ATTACKS AND THE IMPORTANCE OF BEING ZERO-DAY

The professional hackers-for-hire group known as Hidden Lynx, first uncovered in September of 2013, continued their operations in 2014. This group took advantage of a significant zero-day vulnerability (CVE-2014-0332)¹⁰ through a watering-hole-style attack. The attack ultimately opened a backdoor on any computer that visited the compromised site while the watering hole was active, through which subsequent attacks and exfiltration could take place.

Another zero-day vulnerability (CVE-2014-1776) was also discovered in watering-hole attacks against organizations involved with the French Aerospace industry and a variety of Japanese websites. However, we believe these attacks are separate from the Hidden Lynx group, and other actors were involved in their use¹¹.

Another significant watering-hole attack took advantage of a zero-day vulnerability in Adobe Flash (CVE-2014-0515), and coupled it with a specific piece of software produced by a legitimate vendor. This particular attack appears to have been highly targeted, as the target organization would need both pieces of software installed in order for the attack to be successful.

In a different case, a previously undiscovered vulnerability in Microsoft Windows allowed the Sandworm cyberespionage group to deliver malware to targeted organizations¹² including NATO, several Ukrainian and Western European government organizations, energy companies, and telecommunications companies.

The Elderwood platform was first identified in 2012, but continues to be maintained. At the start of 2014, for example, it exploited three new zero-day vulnerabilities to attack its victims¹³.

Twenty-four zero-days were discovered in 2014, consistent with the all-time high of 2013, indicating a new norm in numbers of zero-days being discovered and exploited. There may be many more as yet undiscovered that attackers are keeping to themselves for now.

For an attacker, the value and importance of an exploit for a zero-day vulnerability for an attacker comes in two

ways. First, any unpublished vulnerability has enormous value if it can be exploited by an attacker to gain remote access or perform reconnaissance. Second, an exploit can reap enormous reward by taking advantage of the delay between a vendor becoming aware of the vulnerability and the time taken to provide a patch. It can take several days, weeks, or even months for a patch to be available, and even longer before it is widely deployed.

For the top-five most frequently exploited zero-day vulnerabilities published in 2014, the total number of days between the vendor publication date and the patch date grew to 295 days, up from 19 in 2013. The average time taken between publication and patch also grew to 59 days, up from 4 in 2013. The most frequently exploited zero-day in 2014, CVE-2013-7331, was first identified in 2013, hence its classification; however, its existence was not disclosed to the public until the following year. It was a further 204 days before the vendor was able to publish a patch. The number two and three most frequent zero-day exploits also had long time-to-patch windows of 22 and 53 days, respectively. Both of these windows are larger than the average seen in 2013.

It is this weakness—the window of vulnerability—that the espionage attack groups depend on for their success. For example, a website already compromised to host a watering-hole exploit may stop using a zero-day exploit once the software vendor publishes information about the vulnerability's existence, even though a patch may not yet be available. The attackers may then switch over to using another as-of-yet undiscovered exploit, a further example of the enormous resources at their disposal.

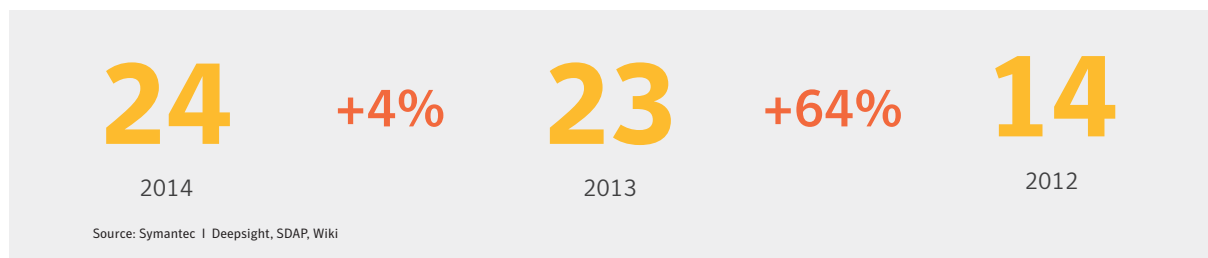
¹⁰ <http://www.symantec.com/connect/blogs/emerging-threat-ms-ie-10-zero-day-cve-2014-0322-use-after-free-remote-code-execution-vulnerabi>

¹¹ <http://www.symantec.com/connect/blogs/zero-day-internet-vulnerability-let-loose-wild>

¹² <http://www.symantec.com/connect/blogs/sandworm-windows-zero-day-vulnerability-being-actively-exploited-targeted-attacks>

¹³ <http://www.symantec.com/connect/blogs/how-elderwood-platform-fueling-2014-s-zero-day-attacks>

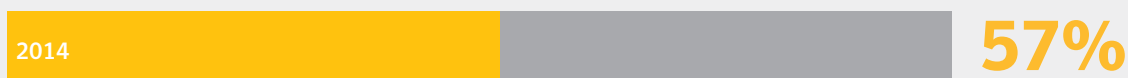
ZERO-DAY VULNERABILITIES



TOP 5 ZERO-DAY VULNERABILITIES, PATCH AND SIGNATURE



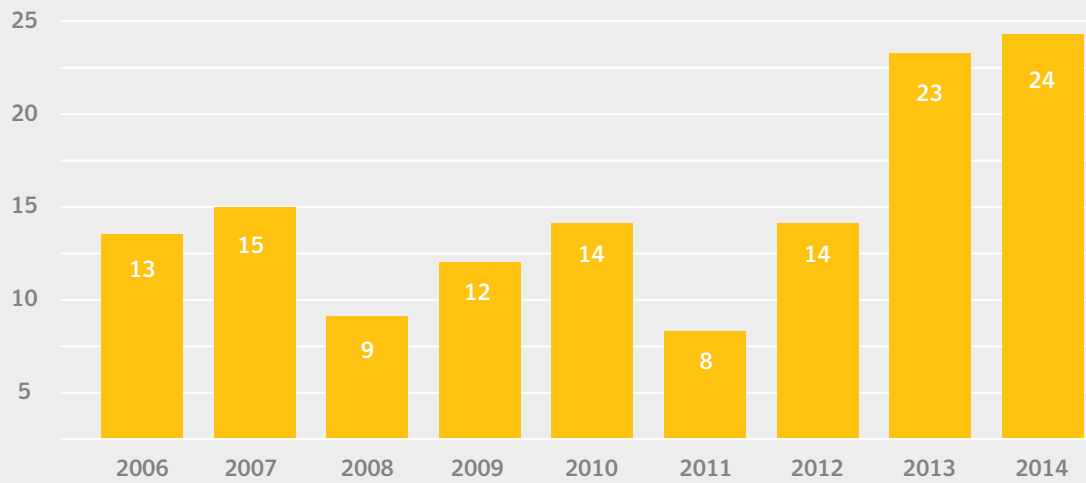
In 2014, 57 percent of all attacks for the top-5 vulnerabilities occurred after a signature was added (under 90 days), and prior to a patch release by the vendor.



RANK	CVE	2014 Overall %
1	Microsoft ActiveX Control CVE-2013-7331	81%
2	Microsoft Internet Explorer CVE-2014-0322	9.5%
3	Adobe Flash Player CVE-2014-0515	7.3%
4	Adobe Flash Player CVE-2014-0497	2.0%
5	Microsoft Windows CVE-2014-4114 OLE	<1%

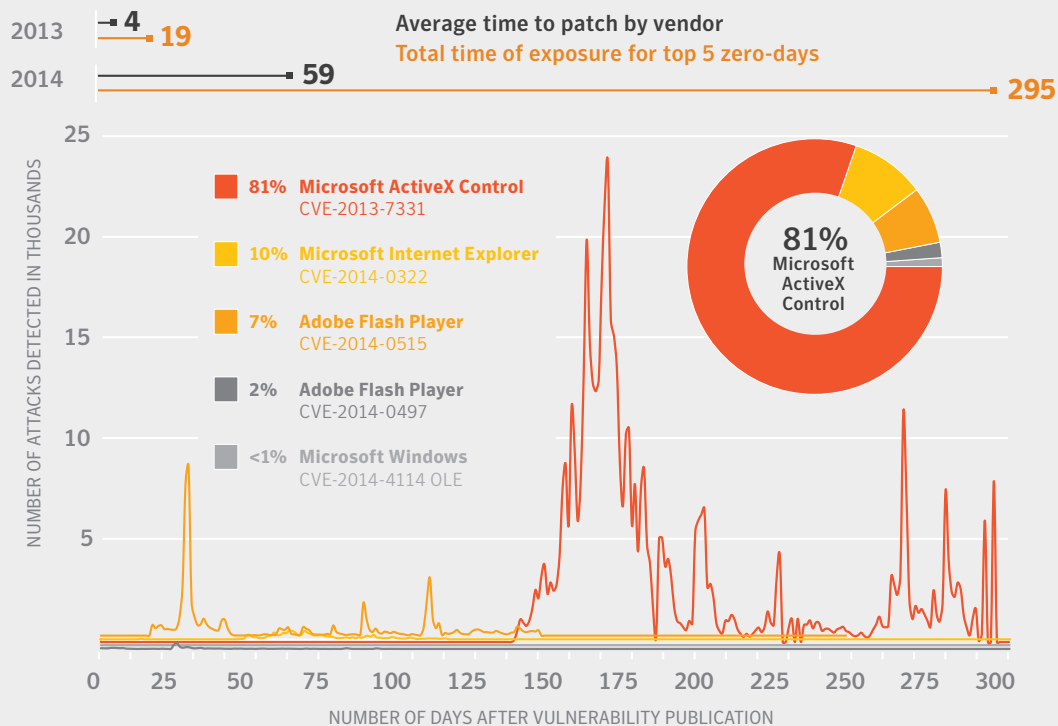
The total number of days between the vendor's publication date and the subsequent patch date, for the top-5 most frequently exploited zero-day vulnerabilities, grew from 19 days in 2013 to 295 days in 2014. 57 percent of the attacks exploiting these top-5 zero-day vulnerabilities were blocked by Symantec Endpoint technology in the first 90 days, often before a patch was made available.

ZERO-DAY VULNERABILITIES, ANNUAL TOTAL, 2006 – 2014



Source: Symantec | SDAP

TOP 5 ZERO-DAY VULNERABILITIES



The window of vulnerability, the duration between the publication date and the patch date, for the most frequently exploited zero-day vulnerabilities grew in 2014. CVE-2014-0322, CVE-2014-0515, and CVE-2014-4114 were all exploited during 2014 in a number of targeted attacks, including attacks related to Hidden Lynx and Sandworm.

THREAT INTELLIGENCE

Threat Intelligence is now a vital component for any organization to understand the potential threats against their networks.

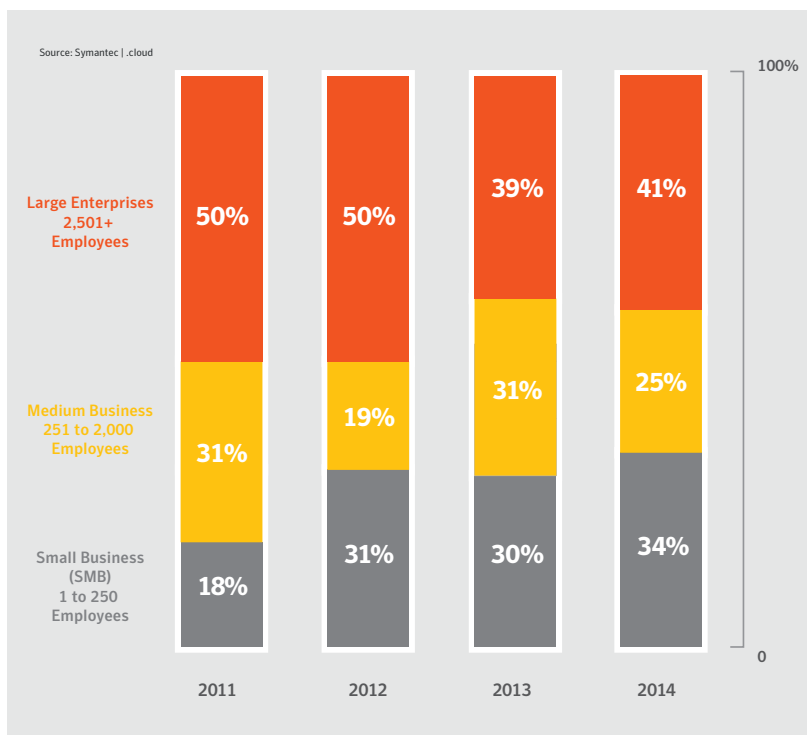
Investing in great technology solves only part of the problem, and a combination of threat intelligence, risk management, and the best technical solutions will help not only to reveal who is being targeted, but also how and why. Understanding the threats is critical, as businesses should now expect to be attacked—the question is not if, but when.

Advanced attackers use exploit toolkits not only against older vulnerabilities, but also new zero-day ones, and being good at defense means being harder to breach. Threat intelligence can provide a prioritized list of suspicious incidents by correlating all available information from across the enterprise. A continual assessment of not only the people and their skills, but also the processes, will ensure the best response is followed, and that processes are continually updated and skills are maintained. If businesses can become harder to breach, the attackers will have to work harder. Don't be the weakest link in the supply chain.



TECHNIQUES USED IN TARGETED ATTACKS

DISTRIBUTION OF SPEAR-PHISHING ATTACKS BY ORGANIZATION SIZE, 2011 –2014



41 percent of spear-phishing emails were directed at Large Enterprises in 2014. As in 2013, spear-phishing attacks on small and medium-size businesses show that being small and relatively anonymous is no protection. In fact, attacks in 2014 confirm that determined attackers often attack a target company's supply chain as a way of outflanking its security.

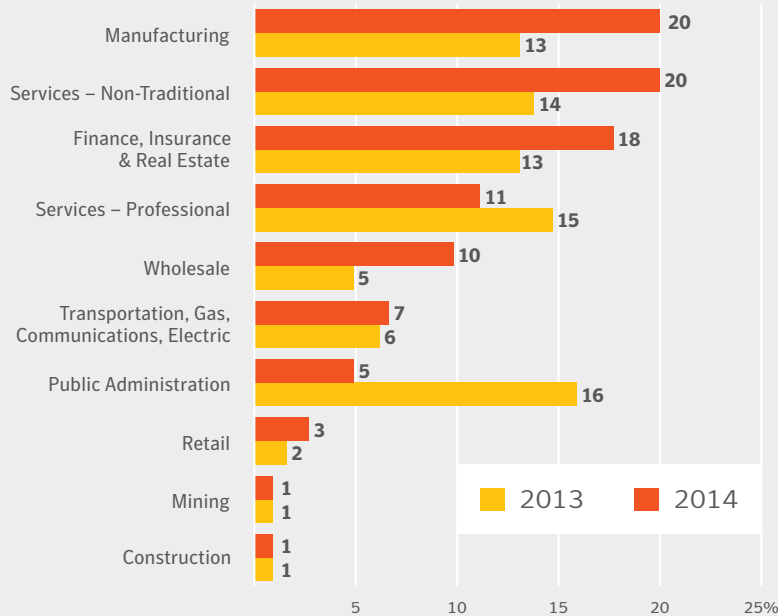
RISK RATIO OF SPEAR-PHISHING ATTACKS BY ORGANIZATION SIZE

Source: Symantec | .cloud, SRL

	2014 Risk Ratio	2014 Risk Ratio as %	2013 Risk Ratio	2013 Risk Ratio as %
Large Enterprises 2,500+ Employees	1 in 1.2	83%	1 in 2.3	43%
Medium Business 251–2,500	1 in 1.6	63%	1 in 3.5	33%
Small Business (SMB) 1–250	1 in 2.2	45%	1 in 5.2	19%

In 2014, 83 percent of large enterprises were targeted in spear-phishing campaigns, compared with 43 percent in 2013.

TOP-TEN INDUSTRIES TARGETED IN SPEAR-PHISHING ATTACKS, 2013–2014



Overall in 2014, the Manufacturing sector was targeted with the greatest volume of spear-phishing attacks, as 1 in 5 (20 percent) were directed at Manufacturing organizations.

Source: Symantec | .cloud

RISK RATIO OF SPEAR-PHISHING ATTACKS BY INDUSTRY

2014 INDUSTRY	2014 Risk Ratio	2014 Risk Ratio as %	2013 Risk Ratio	2013 Risk Ratio	2013 Risk Ratio as %
Mining	1 in 2.3	43%	Mining	1 in 2.7	37%
Wholesale	1 in 2.9	34%	Public Administration (Government)	1 in 3.1	32%
Manufacturing	1 in 3.0	33%	Manufacturing	1 in 3.2	31%
Transportation, Communications, Electric, Gas & Sanitary Services	1 in 3.4	29%	Wholesale	1 in 3.4	29%
Public Administration	1 in 3.4	29%	Transportation, Communications, Electric, Gas & Sanitary Services	1 in 3.9	26%
Finance, Insurance & Real Estate	1 in 4.8	21%	Finance, Insurance & Real Estate	1 in 4.8	21%
Retail	1 in 4.8	21%	Services — Non-Traditional	1 in 6.6	15%
Services - Non Traditional	1 in 6.5	15%	Construction	1 in 11.3	8%
Services - Professional	1 in 6.9	15%	Agriculture, Forestry & Fishing	1 in 12.0	8%

Source: Symantec | .cloud, SRL

The Mining industry was the most heavily targeted in 2014, with 43 percent (1 in 2.3) of mining organizations being targeted at least once during the year. The Mining classification includes energy extraction organizations, as well as those mining metals, and quarrying minerals.



RISK RATIO OF SPEAR-PHISHING ATTACKS BY JOB ROLE

Source: Symantec | .cloud, SRL

2014	2014 Risk Ratio	2014 Ratio as %
Sales/Marketing	1 in 2.9	35%
Operations	1 in 3.8	27%
Finance	1 in 3.3	30%
R&D	1 in 4.4	23%
IT	1 in 5.4	19%
Engineering	1 in 6.4	16%
HR & Recruitment	1 in 7.2	14%
Other	1 in 9.3	11%

Individuals in Sales and Marketing job roles were the most targeted in 2014, with 1 in 2.9 of them being targeted at least once; this is equivalent to 35 percent of Sales and Marketing personnel.

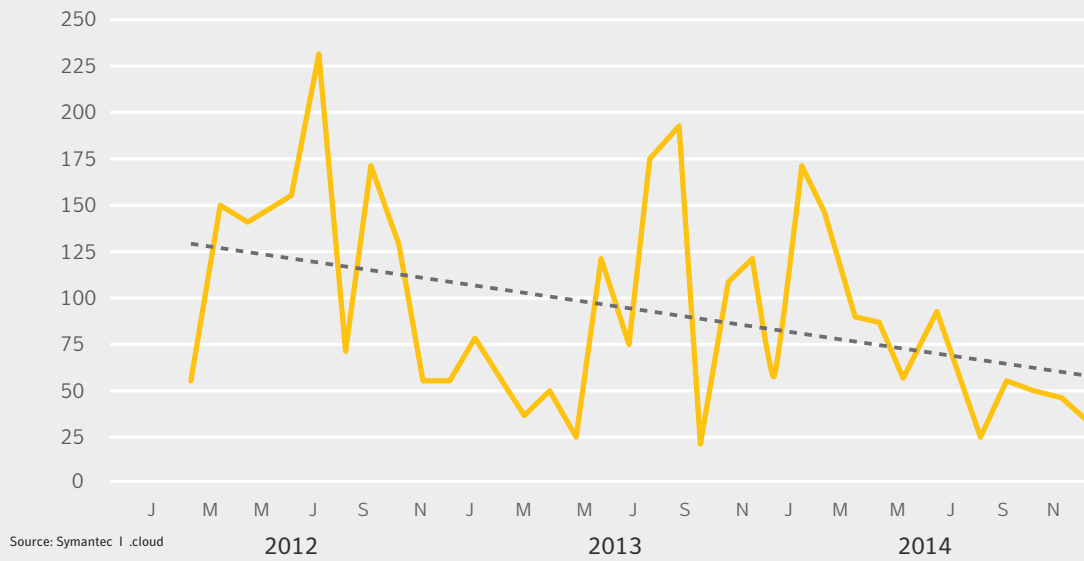
RISK RATIO OF SPEAR-PHISHING ATTACKS BY JOB LEVEL

Source: Symantec | .cloud, SRL

2014	2014 Risk Ratio	Risk Ratio as %
Manager	1 in 3.8	26%
Individual Contributor	1 in 3.7	27%
Intern	1 in 3.9	26%
Director	1 in 5.4	19%
Support	1 in 7.6	13%
Other	1 in 9.3	11%

Managers were the most frequently targeted level of seniority in 2014, with 1 in 3.8 of them being targeted at least once; this is equivalent to 26 percent of individuals at managerial level.

AVERAGE NUMBER OF SPEAR-PHISHING ATTACKS PER DAY, 2012-2014



ANALYSIS OF SPEAR-PHISHING EMAILS USED IN TARGETED ATTACKS, 2013 – 2014

Rank	Executable Type	2014 Overall %	Executable Type	2013 Overall %
1	.doc	41.2%	.exe	31.3%
2	.exe	24.0%	.scr	18.4%
3	.scr	9.7%	.doc	7.9%
4	.au3	8.7%	.pdf	5.3%
5	.jpg	4.9%	.class	4.7%
6	class	3.6%	.jpg	3.8%
7	.pdf	3.3%	.dmp	2.7%
8	.bin	2.0%	.dll	1.8%
9	.txt	1.5%	.au3	1.7%
10	.dmp	1.1%	.xls	1.2%

Office document file attachments overtook executable files to become the most frequently used tactic for attachments used in spear-phishing attacks, used in 41 percent of attacks during 2014. At least 35 percent of spear-phishing attacks could be prevented if companies blocked executable-type file attachments and screensavers at the email gateway. Malicious document attachments could also be rendered safe before reaching the email gateway through the use of strong cloud-based filtering that can identify and eliminate spear-phishing attacks before reaching the corporate network.

Source: Symantec | .cloud

SECURING INDUSTRIAL CONTROL SYSTEMS

by Preeti Agarwal

Targeted attacks have evolved from novice intrusion attempts to become an essential weapon in cyberespionage. Industrial control systems (ICS) are prime targets for these attackers, with motives for executing attacks at a national security level. These trends are leading countries to reinforce their investment and build strategies to improve ICS security.

The term “industrial control system” refers to devices that control, monitor, and manage critical infrastructure in industrial sectors, such as electricity, water and wastewater, oil and natural gas, transportation, etc. Various types of ICSes include supervisory control and data acquisition (SCADA), programmable logic controllers (PLC), distributed control systems (DCS), to name a few.

Attacks targeting ICSes have become a common occurrence, and can potentially have serious social and economic impacts. But these attacks often go undisclosed, limiting the PR fallout for the victim, and underreporting the extent of the problem.

There have been numerous attacks, with intentions ranging from cyberespionage to damaging the utilities in ICSes. In 2010 Stuxnet was discovered, a threat designed to attack specific SCADA systems and damage the physical facilities of Iran’s nuclear system. Since then a myriad of weaponized malware has been seen in the threat landscape, and 2014 was no exception. The attackers behind Dragonfly, a cyberespionage campaign against a range of targets, mainly in the energy sector, managed to compromise a number of strategically important ICSes within these organizations and could have caused damage or disruption to the energy supply in the affected countries, had they used the sabotage capabilities open to them.

More recently, Sandworm launched a sophisticated and targeted malware campaign compromising the human-machine interface (HMI) of several well-known ICS vendors. Attackers used the internet-connected HMIs to exploit vulnerabilities in the ICS software. Such intrusions could have been reconnaissance for another attack.

The most recent addition to emerge in 2014 was an incident where a blast furnace at a German steel mill suffered massive damage following a cyber-attack on the plant’s network¹⁴.

Attacks against ICSes have matured and become more frequent, making the security of these systems essential and a pressing issue.

Many ICSes are installed and operate for many years. This often leads to security policies rooted in a security-through-obscure approach, using physical isolation, proprietary protocols, and specialized hardware in the hopes that this will keep them secure. Many of these systems were developed before Internet-based technologies were used in businesses, and were designed with a focus on reliability, maintainability, and availability aspects, with little-or-no emphasis on security. However, compelling needs for remote accessibility and corporate connectivity have changed the attack surface dramatically, exposing new vulnerabilities in these systems to attacks.

The primary entry point for these attacks today is poorly protected Internet-accessible, critical infrastructure devices. In order to provide remote accessibility, elements of SCADA systems, used to monitor and control the plants and equipment, are connected to the Internet through corporate networks. These SCADA elements expose the control network and pose a risk of attacks like scanning, probing, brute force attempts, and unauthorized access of these devices.

One way to leverage these devices in an attack is through the HMI, often accessible from the corporate network. An attacker can compromise the corporate hosts by exploiting any existing zero-day vulnerability, discover

¹⁴ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

any hosts that have access into the control network, and attempt to leverage this information as a way into the ICSes.

Another way to leverage ICSes is through an HMI connected directly to the Internet. These Internet-facing devices can be easily discovered over the Internet using common search engines. Once a control device is identified, it can be compromised by exploiting vulnerabilities or through an improper configuration. The level of knowledge required for launching these attacks is fairly low.

Apart from these entry points, ICSes and their software have several inherent vulnerabilities, opening doors for adversaries. Many of the proprietary Web applications available have security vulnerabilities that allow buffer overflows, SQL injection, or cross-site scripting attacks. Poor authentication and authorization techniques can lead the attacker to gain access to critical ICS functionalities. Weak authentication in ICS protocols allows for man-in-the-middle attacks like packet replay and spoofing. An attacker can end up sending rogue commands to PLCs, or fake status to HMIs.

Ladder logic used to program the PLCs is a critical asset in ICS environments. Compromises to an engineering work station used for developing and uploading this PLC ladder logic can lead to reverse engineering, which can be used to craft attacks.

Securing ICS environments requires a comprehensive security plan that would help an organization define its security goals in terms of standards, regulatory compliance, potential risk factors, business impacts, and required mitigation steps. Building a secure ICS environment requires integrating security into each phase of the industrial processes starting from planning to the day-to-day operations.

Network-level segregation between the control network and corporate network should be an absolute requirement as it greatly reduces the chances of attacks originating from within corporate networks. However practical considerations require ICS connectivity from the corporate network. In such cases the access points should be limited, protected by a firewall, and should make use of trusted communication channels like a VPN.

ICS environments are evolving, with vendors extending support for security software on the control devices for general-purpose SCADA servers and engineering workstations. However systems like PLCs and DCSes still use vendor-specific customized operating systems. These control systems, once installed, have zero tolerance for downtime, limited resources and time-dependent code. This limits opportunities to deploy traditional enterprise-security solutions designed for IT computer systems. Given these challenges there is no silver bullet solution for ICS security. Rather security has to be implemented end-to-end at each layer, including the network perimeter, access points within the corporate and external network, the network level, and host-based and application-levels.

In addition, the control devices themselves should also be secure by design. Manufacturers are responsible to ensure that security is built into the control devices before shipping.

Looking ahead, we will likely see a trend towards an increase in the use of mobile technology allowing remote HMI access and control options. While the solution is very compelling from administrative efficiency perspective, it will launch a new attack surface associated with the mobile usage model.

It's also possible that we will see the development of generalized techniques for attacking ICSes. As a result we may see a rise in freely available ICS exploit kits. This trend would no doubt increase ICS attack numbers.

As we saw with Stuxnet, which reincarnated itself with multiple variants, ICS-focused threats that followed had similarities in attack vectors and artifacts, making use of common ICS protocols and general-purpose Trojans. It is highly likely that there are threats out there on ICSes, installed stealthily, that have not yet been detected, sitting passively at the moment. Attackers may find a reason to make these passive attacks active at any point in time. It's entirely possible that we will see an onset of more critical infrastructure vulnerabilities being utilized, to dangerous ends.

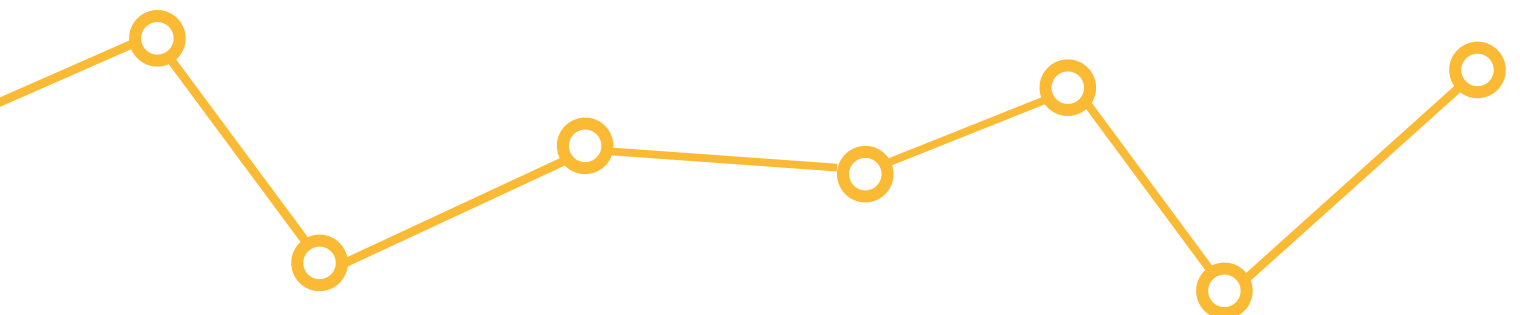
DATA BREACHES

The logo for WSTR is centered within a dark grey rectangular box with a white border. The letters 'W', 'S', and 'R' are rendered in a white, outlined, sans-serif font. The letter 'T' is rendered in a solid, bold, orange sans-serif font. A white line with circular nodes at its ends passes behind the box, extending from the left edge to the right edge of the page.

WSTR

AT A GLANCE

1	2014 saw fewer mega breaches (with more than 10m identities disclosed) than 2013
2	Overall number of data breaches increased
3	At 49 percent, attackers are responsible for the majority of breaches
4	Attacks on point-of-sale systems have grown in scale and sophistication
5	According to a survey carried out by Symantec, 57 percent of respondents are worried their data is not safe



INTRODUCTION

In 2014, cybercriminals continued to steal private information on an epic scale, by direct attack on institutions such as banks and from retailers' point-of-sale systems.

In 2014, JPMorgan Chase, an American bank, acknowledged that data associated with 83 million accounts—76 million households and 7 million small businesses—was compromised in one of the largest data breaches in history¹⁵.

In September 2014, Home Depot suffered a data breach of 56 million credit card numbers. Criminals continued to target retail point-of-sale systems and, in one attack, Staples saw a million customer payment card records stolen¹⁶. However, many breaches—perhaps the majority—go unreported or undetected^{17,18}.

The release of nearly 200 celebrity photographs on the website 4chan in August 2014 received wide media coverage and increased consumer anxiety about privacy.

According to Apple, the images were obtained using highly tailored targeted attacks on individual accounts, rather than general weaknesses in the company's security¹⁹.

2014 saw fewer 'mega breaches' than 2013, although the total number of breaches did increase by 23 percent. People's personal and financial information continues to command high prices on the black market, and that means that cybercriminals will continue to target major institutions for large scores and small companies for easy ones. Many breaches are preventable with the right security measures, including elements such as data loss prevention, encryption, and intrusion detection systems, as well as effective security policies and training.

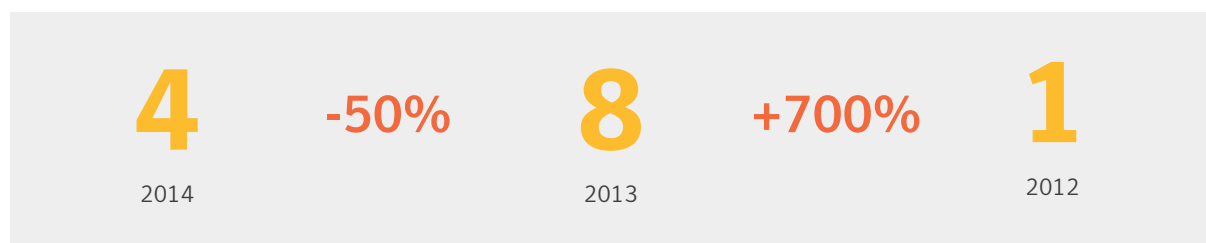
TOTAL BREACHES

Source: Symantec | CCI



BREACHES WITH MORE THAN 10 MILLION IDENTITIES EXPOSED

Source: Symantec | CCI



While 2014 had fewer mega breaches (greater than 10M identities exposed per breach), the total number of breaches remained at the high level first established in 2013, suggesting we have entered a new era of breach activity.

¹⁵ <http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003>

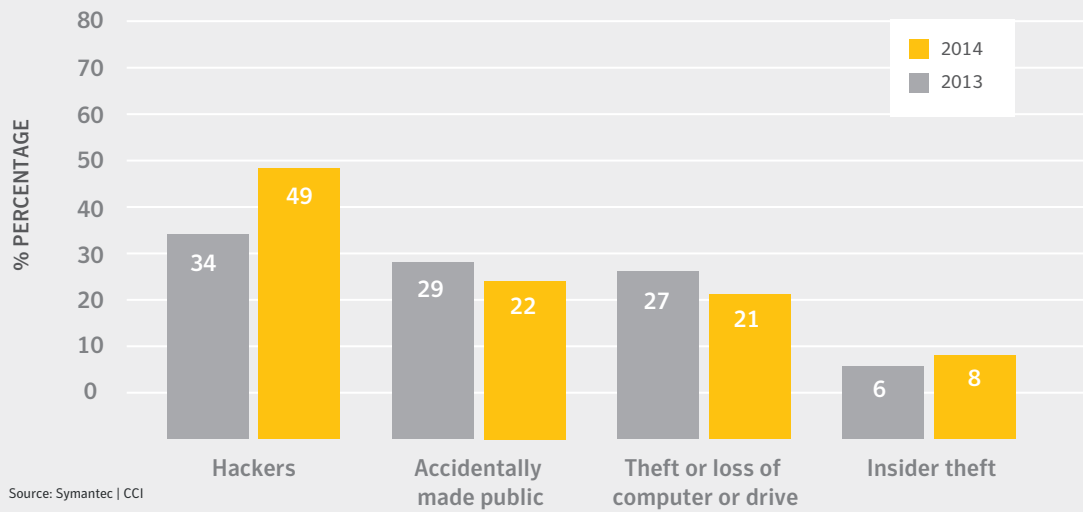
¹⁶ <http://staples.newshq.businesswire.com/press-release/corporate/staples-provides-update-data-security-incident>

¹⁷ <http://www.insurancejournal.com/news/west/2014/03/07/322748.htm>

¹⁸ <http://www.ponemon.org/news-2/7>

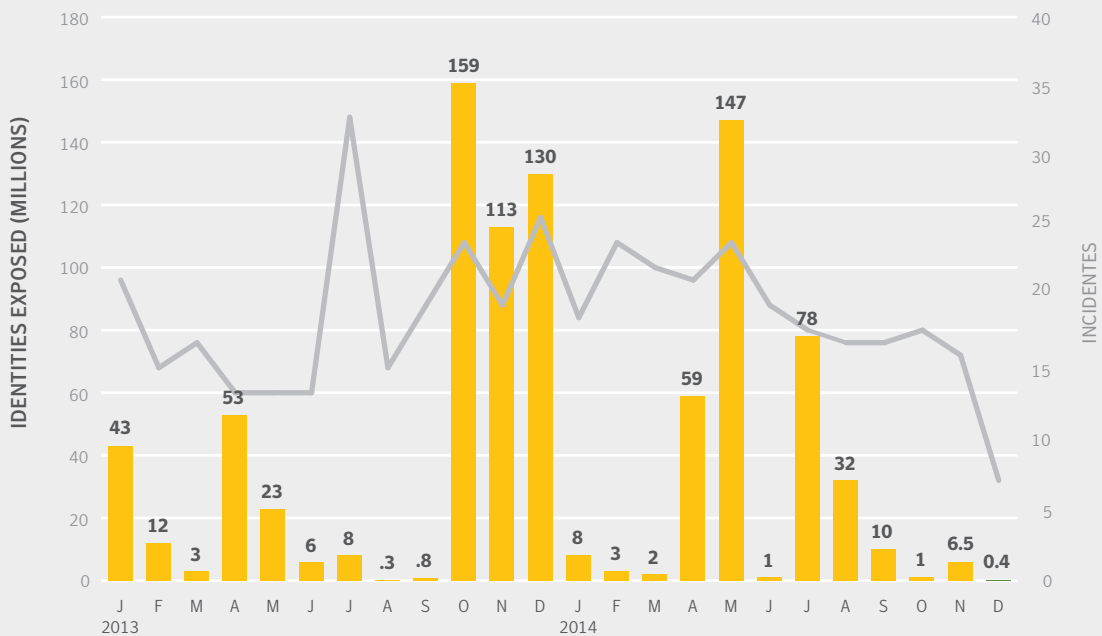
¹⁹ <https://www.apple.com/uk/pr/library/2014/09/02Apple-Media-Advisory.html>

TOP CAUSES OF DATA BREACHES, 2013 - 2014



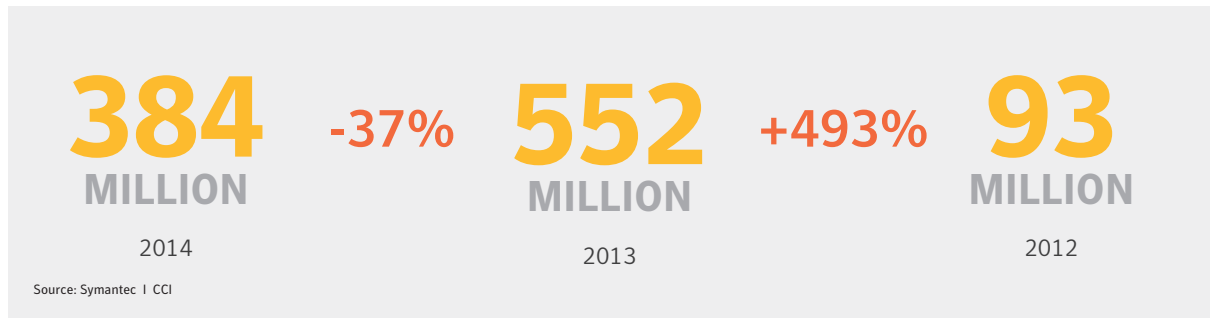
At 49 percent, the majority of breaches were caused by attackers, up from 34 percent in 2013. However, a further 22 percent of breaches were classified as Accidentally Made Public, and 21 percent were due to Theft or Loss of a Computer or Drive. These latter types of data exposure are preventable if data is encrypted, effectively eliminating the impact of the data falling into the wrong hands. The good news is that this figure is down from 56 percent in 2013.

TIMELINE OF DATA BREACHES, 2013 – 2014

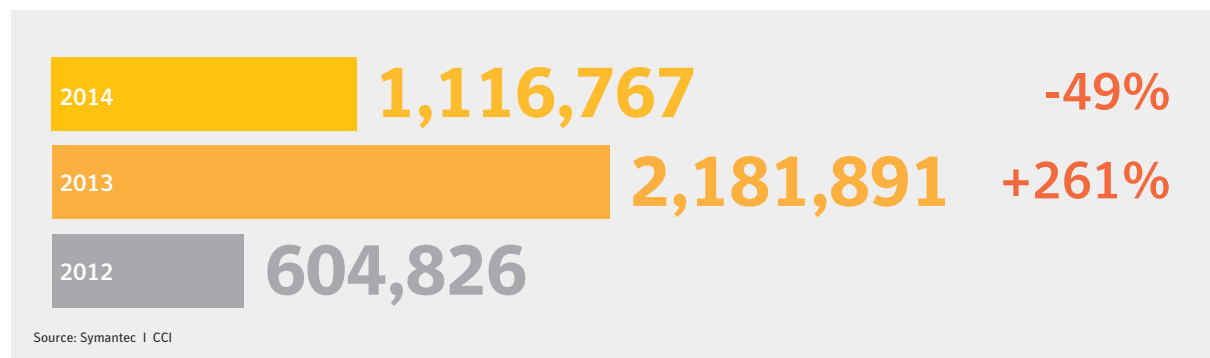


One significant downturn in 2014 is the number of identities exposed as the result of a data breach. In 2013, we reported that there were 552 million identities exposed. In 2014, this appears to be down significantly, at 348 million identities.

TOTAL IDENTITIES EXPOSED



AVERAGE IDENTITIES EXPOSED / BREACH



MEDIAN IDENTITIES EXPOSED / BREACH



On the surface, this looks like there were far fewer identities exposed. The fact that there were fewer breaches reported containing more than 10 million identities plays a part in this drop, if anything for sheer volume of identities. It is also possible that large organizations sat up and took notice of the major breaches that occurred towards the end of 2013, implementing security policies that reduced the risk of a data breach, such as rolling out a Data Loss Prevention (DLP) solution that prevents most data from being exfiltrated, even if attackers succeed in penetrating the network.

While these items no doubt played a part, our numbers point to another possibility: the number of organizations that are withholding information on the number of identities exposed is increasing. In 2013, we recorded 34 out of 253 breaches, or 13 percent, where the number of identities exposed was not disclosed. In comparison, 61 out of 312, or 20 percent of breaches disclosed in 2014, didn't include this information. This equates to 1 in 5 breaches not reporting on the breadth of data exposed in a breach.

It's difficult to definitively explain why this information is not being shared publicly. In some cases, it's possible the organizations find it too challenging to determine the number of identities that were exposed. In others, this information likely remains undisclosed to help save face in what clearly has a negative impact on the organization's public reputation.

What is most concerning, however, is that this trend could point to a situation where a large number of breaches are not being disclosed to the public at all. While there are many industries, such as healthcare and some government organizations, where a breach must be reported by law, most industries do not. As a result, some organizations may decide to withhold information about a breach to protect the company's reputation, and do not face penalties as a result. This may change in the coming years, as many governing agencies around the world are already looking at bringing in regulation surrounding the proper disclosure of data breaches.

TOP-TEN SECTORS BREACHED BY NUMBER OF INCIDENTS

Source: Symantec | CCI

Rank	Sector	Number of Incidents	% of Incidents
1	Healthcare	116	37.2%
2	Retail	34	10.9%
3	Education	31	9.9%
4	Government and Public Sector	26	8.3%
5	Financial	19	6.1%
6	Computer software	13	4.2%
7	Hospitality	12	3.8%
8	Insurance	11	3.5%
9	Transportation	9	2.9%
10	Arts and media	6	1.9%

TOP-TEN TYPES OF INFORMATION EXPOSED

Source: Symantec | CCI

Rank	2014 Type	2014 %	2013 Type	2013 %
1	Real Names	68.9%	Real Names	71.5%
2	Gov ID numbers (Soc Sec)	44.9%	Birth Dates	43.1%
3	Home Address	42.9%	Government ID (Soc Sec)	39.5%
4	Financial Information	35.5%	Home Address	37.5%
5	Birth Dates	34.9%	Medical Records	33.6%
6	Medical Records	33.7%	Phone Numbers	19.0%
7	Phone Numbers	21.2%	Financial Information	17.8%
8	Email Addresses	19.6%	Email Addresses	15.4%
9	Usernames & Passwords	12.8%	User Names & Passwords	11.9%
10	Insurance	11.2%	Insurance	5.9%

Real Names, SSN and Home address were among the top-three type of information breached in 2014. The exposure of financial information grew from 17.8 percent to 35.5 percent in 2014, the largest increase within the top-ten list of information types exposed.

RETAILERS UNDER ATTACK

Attackers clearly have retailers in their cross hairs, if the increase in data breaches containing financial information is any indication. The Retail industry again has the dubious distinction of being the industry most liable for large numbers of identities exposed, comprising almost 60 percent of all identities reported exposed, up from 30 percent in 2013. Financial information has moved to the fourth most common type of information exposed in a breach. In 2013, 17.8 percent of breaches contained financial information, but in 2014 this number jumped to 35.5 percent.

TOP-TEN SECTORS BREACHED BY NUMBER OF IDENTITIES EXPOSED

Source: Symantec | CCI

Rank	Sector	Number of Identities Exposed	% of Identities Exposed
1	Retail	205,446,276	59.0%
2	Financial	79,465,597	22.8%
3	Computer software	35,068,405	10.1%
4	Healthcare	7,230,517	2.1%
5	Government and Public Sector	7,127,263	2.0%
6	Social networking	4,600,000	1.3%
7	Telecom	2,124,021	0.6%
8	Hospitality	1,818,600	0.5%
9	Education	1,359,190	0.4%
10	Arts and media	1,082,690	0.3%

This financial information can range from bank account details to tax related documents, but in most cases this information is credit or debit card details. Online retailers play a significant part, but what is appearing more often in the data breaches reported is attacks on point-of-sale systems: the credit card swipe machines that have become so ubiquitous in our retail lives.

Although the first attacks on retail point-of-sale systems date back to 2005, Symantec saw an upsurge in attacks in 2014. It is now one of the biggest sources of stolen payment card data²⁰, and is behind some of 2013 and 2014's biggest data breaches.

Point-of-sale systems are made vulnerable by a widespread lack of security, including poor or non-existent encryption of data, software vulnerabilities, reliance on out-of-date software such as Microsoft Windows XP, which went out of support in 2014, and the slow adoption of 'chip-and-pin' technology outside Europe. With new ways to pay, such as Apple Pay and chip-and-pin cards coming to the US, point of sale data should become more secure over the next few years.

They are likely to remain a top target for attacks in the near term. Credit card companies are quick to spot anomalous spending patterns, as are observant card owners. This means that criminals need a steady supply of 'fresh' card numbers and the online economy provides a ready market of buyers and sellers²¹.

²⁰ http://securityresponse.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/attacks_on_point_of_sale_systems.pdf

²¹ <http://www.symantec.com/connect/blogs/demystifying-point-sale-malware-and-attacks>

PRIVACY AND THE IMPORTANCE OF DATA SECURITY

The prevalence of data breaches over the last number of years has certainly had an impact on consumer's views concerning their private information. Symantec carried out a survey on the topic of privacy within the European Union, publishing some interesting findings in the State of Privacy Report 2015²².

For instance, of those surveyed, 59 percent of respondents have experienced a data-protection issue in the past. These issues not only include being notified of a data breach by a company that they use, but also an email account being hacked, bank details stolen, online identify theft, a computer virus, social media account hack, or responding to an online scam or fake email.

Overall, 57 percent of respondents are worried their data is not safe. This is no small matter, as data security is very important to consumers, considering that 88 percent say this is an important factor when choosing a company to do business with—more important than the quality of the product (86 percent) or the customer service experience (82 percent).

On top of that, only 14 percent of respondents were happy to share their data with third parties, with 47 percent being unhappy to share any data, and 35 percent requiring some form of check on exactly what data was shared.

Those surveyed also indicated that they are actively adopting a self-moderation approach to their personal data, and taking the matter in to their own hands. According to Symantec's research, over half of those surveyed (57 percent) are now avoiding posting personal details online. Another popular approach to self-moderation could also have chilling repercussions for business, as 1 in 3 consumers admitted they provide false information in order to protect their privacy.

On another note, attackers have become more patient, breaching organizations' defenses and lying in wait, building-up knowledge of the patterns of behavior from activity on the network: learning who does what and how. This way, they are better able to not only target them, but impersonate and exploit them. It is through the use of legitimate, stolen credentials, and the level of patience required in conducting such attacks, as opposed to springing an attack immediately following a breach. By carefully monitoring these cycles of behavior for a long time, these attacks can appear like normal patterns of behavior.

The traditional perimeter for an organization is no longer as clear as it once was—the boundaries are blurred—and mobile devices make this especially more difficult to manage. Data is also stored not only on mobile devices, but increasingly in the cloud. Mobile devices have become the key to accessing this data since passwords are more likely to be cached on mobile devices, which moreover are less likely to be encrypted than a stolen laptop.

²² <http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf>

DATA BREACHES IN THE HEALTHCARE INDUSTRY

by Axel Wirth

Driven by market forces and the desire to improve health delivery, reduce cost, and to comply with government mandates, healthcare providers have been adopting electronic records and digital clinical systems in record numbers. In addition, an aging population requiring management of chronic diseases, new diagnostic methodologies delivering higher quality results, as well as an increasing number of covered patients are leading to rapidly growing data volumes.

All this is leading to a more complex IT infrastructure, increasing needs for integration and exchange of information, new care delivery and reimbursement models, and the accumulation of data. These combined trends are making the healthcare industry more attractive to attackers, and has put providers at an increasing risk of data breaches, both intentional and accidental.

2014 saw a 23 percent increase in the number of healthcare data breaches. Unlike data breaches as a whole, human error and device theft—related or unrelated to the data present—still make up the majority of these incidents. Lost or stolen devices are accountable for the largest portion of breaches in the healthcare industry. According to the Norton Cybercrime Index, 45 percent of healthcare breaches were the result of lost or stolen devices, a 10 percent increase over the previous year. Identities being accidentally exposed publically as the result of error is also up approximately 11 percent in 2014.

However, targeting patient medical information for purposes of medical identity theft, financial fraud, or health insurance fraud has become an increasing problem. Specifically interested in personal identifiable information (PII) or protected health information (PHI), thieves appear to have more incentive to either hack into healthcare organizations or attempt to hire insiders to obtain electronic copies or printouts of patient records. In fact, the number of data breaches in the healthcare industry that were the result of insider theft has more than doubled in 2014. Data breaches that are the result of hacking are up 82 percent in 2014.

More advanced attacks may target larger volumes of electronic records for identity theft, such as in the retail sector. There are also other criminal activities including extortion, blackmail, or celebrity snooping. However, an unprecedented number of cases have been reported around the globe and across all types of healthcare organizations, from large academic medical centers to small community hospitals, when compared to any other industry. Neither location nor size provide any protection, as in the case of a rural, 22-bed community hospital in Southern Illinois, which received stolen patient data in an email with the request to pay a ransom, or the information would be made public²³.

A number of hospitals have mature cybersecurity programs in place, but many are still struggling with basic goals like implementing encryption to protect data on lost or stolen mobile devices, laptops, or data carriers. Too many healthcare organizations are still underinvesting in cybersecurity, making them an easy target for cybercriminals' increasingly sophisticated and targeted attacks.

Unfortunately, for the most part the healthcare industry is not prepared to face today's cyber security risks, no matter if they are hospitals, pharmaceutical or biotech companies, medical device manufacturers, health insurers, national health agencies, or employers.

Many organizations, such as the SANS Institute, US Department of Homeland Security, FBI, and FDA have all issued dire warnings about the cybersecurity risks to the healthcare industry. Nor is it just a US-centric issue, as breaches were reported in many other countries.

²³ "Illinois hospital reports data blackmail"; PC World; Dec. 15, 2014; <http://www.pcworld.com/article/2859952/illinois-hospital-reports-data-blackmail.html>

There is a thriving underground market for medical information and criminals are monetizing it in many ways and for many reasons.

First, medical data sets tend to be more complete when compared to what can be obtained elsewhere. It includes demographics, government ID numbers, bank & credit card accounts, insurance plan credentials, disease statuses, and physical descriptors. This data can be used for identify theft, financial fraud, prescription fraud, obtaining medical services, or reselling the data on the black market. Physical characteristics of patients could be misused to obtain passports, visas, or other forms of identity cards²⁴. In short, it is enticing for malicious agents due to the breadth and depth of the data.

Medical identity theft has been shown to be much more costly to the victims in ways other than just financial. Incorrect data in your medical records may lead to incorrect or delayed diagnoses or treatments, could affect job prospects, and are generally difficult to correct. Unlike financial fraud, where consumers have limited liability, there is little protection against healthcare fraud and the long-term consequences²⁵.

Where credit card numbers may fetch \$0.50 to \$1 in the underground economy, basic identity and insurance information can be valued up to \$10²⁶ or even as high as \$50²⁷, based on its completeness, which may even include ready-made insurance membership cards, driver's licenses, and credit cards.

Breach numbers in healthcare are high, and they are trending up. Traditionally, device loss or theft has been the predominant challenge for healthcare organizations, but we are now seeing an increase in targeted attacks on healthcare organizations, resulting in breaches with a significant impact on healthcare providers and patients. Overall unintentional causes, such as losing devices or accidentally exposing data, are still the most common reason, but breaches caused by malicious actors, such as attackers or insider theft, are increasing far more rapidly. This trend highlights the need for healthcare organizations to ensure there are processes in place to handle theft or loss, but also policies in place to protect against outside agents attempting to gain access to lucrative data.

²⁴ "Medical identity theft proves lucrative in myriad ways"; Fierce Health IT; Oct. 21, 2014; http://www.fiercehealthit.com/story/medical-identify-theft-proves-lucrative-myriad-ways/2014-10-21?utm_medium=nl&utm_source=internal

²⁵ "The Growing Threat of Medical Identity Fraud: A Call to Action"; Medical Identity Fraud Alliance (MIFA); July 2013; <http://medidfraud.org/wp-content/uploads/2013/07/MIFA-Growing-Threat-07232013.pdf>

²⁶ "Your medical record is worth more to hackers than your credit card"; Reuters; Sept. 24, 2014; <http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924>

²⁷ "Stolen EHR Charts Sell for \$50 Each on Black Market"; MedScape; April 18, 2014; <http://www.medscape.com/viewarticle/824192>

RECOMMENDATIONS AND BEST PRACTICE

The logo for WSTR is centered within a dark grey rectangular box with a white border. The letters 'W', 'S', and 'T' are rendered in a white, outlined, sans-serif font. The letter 'R' is rendered in a solid, bold, sans-serif font with a yellow-to-orange gradient. A white line with circular nodes at its ends passes behind the box, extending from the left edge to the right edge of the page.

WSTR



Despite this year's vulnerabilities, when it comes to protecting your website visitors and the information they share with you, SSL and TLS remain the gold standard. In fact, due to the publicity that Heartbleed received, more companies than ever have started hiring SSL developers to work on fixes and code. This has made for more eyes on the SSL libraries and common good practices in implementation.



Get Stronger SSL

2014 saw SSL certificate algorithms become stronger than ever. Symantec, along with several other CAs, have moved to SHA-2 as default, and is winding down support for 1024-bit rootsⁱ.

Microsoft and Google announced SHA-1 deprecation plans that may affect websites with SHA-1 certificates expiring as early as January 1, 2016ⁱⁱ. In other words, if you haven't migrated to SHA-2, visitors using Chrome to access your site will likely see a security warning, and as of January 1, 2017, your certificates just won't work for visitors using IE.

Symantec is also advancing the use of the ECC algorithm—a much stronger alternative to RSA. All major browsers, even mobile, support ECC certificates on all the latest platforms, and there are three main benefits to using it:

1. Improved security. Compared to an industry-standard 2048-bit RSA key, ECC-256-bit keys are 10,000 times harder to crackⁱⁱⁱ. In other words, it would take a lot more computing power and a lot longer for a brute force attack to crack this algorithm.

2. Better performance. Website owners used to worry that implementing SSL certificates would slow their site down. This led to many sites having only partial-on SSL, which creates serious vulnerabilities. ECC requires much less processing power on the website than RSA, and can handle more users and more connections simultaneously. This makes the implementation of Always-on SSL not only sensible, but viable too.

3. Perfect Forward Secrecy (PFS). Although PFS is an option with RSA-based and ECC-based certificates, performance is much better with ECC-based certificates. Why does that matter? Well, without PFS, if a hacker got hold of your private keys, they could retrospectively decrypt any and all data they had captured. Considering the Heartbleed vulnerability made this a very real possibility for so many websites, this is a problem. With PFS, however, if a hacker cracks or gets hold of your SSL certificate private keys, they can only decrypt information protected with those keys from that point on. They can't decrypt any historical data.



Use SSL Right

As we've seen from 2014, SSL is only as good as its implementation and maintenance. So be sure to:

- **Implement Always-on SSL.** Use SSL certificates to protect every page of your website, so that every interaction a visitor has with your site is authenticated and encrypted.
- **Keep servers up to date.** This applies beyond server SSL libraries: any patch or update should be installed as soon as possible. They're released for a reason: to reduce or eliminate a vulnerability.
- **Display recognized trust marks** (such as the Norton Secured Seal) in highly visible locations on your website to show customers your commitment to their security.
- **Scan regularly.** Keep an eye on your web servers and watch for vulnerabilities or malware.
- **Keep server configuration up to date.** Make sure that old, unsecure versions of the SSL protocol (SSL2 and SSL3) are disabled, and newer versions of the TLS protocol (TLS1.1 and TLS1.2) are enabled and prioritized. Use tools like Symantec's SSL Toolbox to verify proper server configuration^{iv}.

ⁱ <http://www.symantec.com/page.jsp?id=1024-bit-certificate-support>

ⁱⁱ <http://www.symantec.com/en/uk/page.jsp?id=sha2-transition>

ⁱⁱⁱ <http://www.symantec.com/connect/blogs/introducing-algorithm-agility-ecc-and-dsa>

^{iv} <https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp>



Educate Employees

Basic common sense and the introduction of some good security habits can go a long way to keeping sites and servers safe this year:

- Ensure employees don't open attachments from senders they don't know
- Educate them on safe social media conduct: offers that look too good, are; hot topics are prime bait for scams; not all links lead to real login pages.
- Encourage them to adopt two-step authentication on any website or app that offers it
- Ensure they have different passwords for every email account, applications, and login—especially for work-related sites and services
- Remind them to use common sense—having anti-virus software doesn't mean it's ok to go on malicious or questionable websites

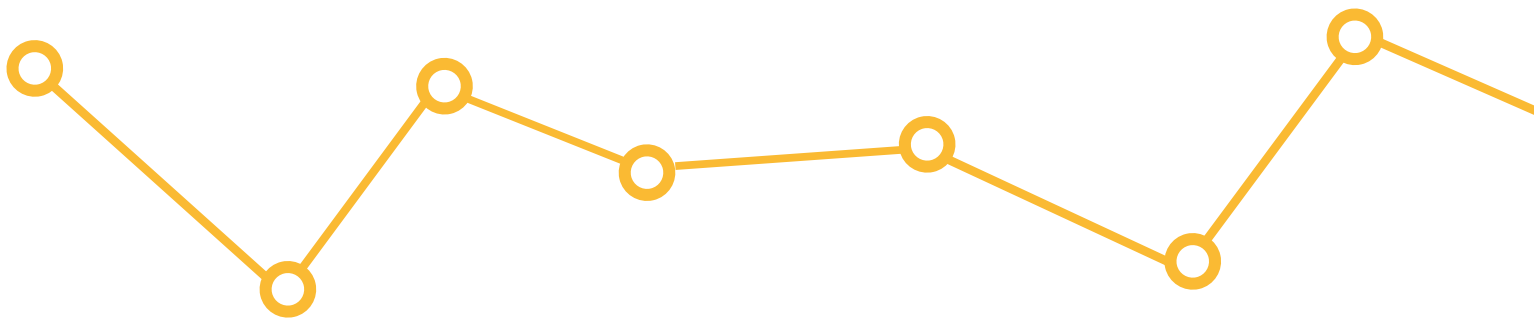


Get Safe or Get Shamed

Attackers have become more aggressive, more sophisticated, and more ruthless than ever in their attempts to exploit the Internet for ill gains. There is, however, plenty individuals and organizations can do to limit their impact.

SSL and website security is now in the public consciousness, and if you're not doing your part, you could find yourself being publicly shamed on HTTP Shaming, a site set up by software engineer, Tony Webster⁹.

When it comes to businesses and their websites, good security processes and implementations are all that stand in the way of total ruin: financial and reputational. So get secure in 2015 with Symantec.



⁹ <http://arstechnica.com/security/2014/08/new-website-aims-to-shame-apps-with-lax-security/>

COMING NEXT

PART 3: SOCIAL MEDIA AND SCAMS

The logo for WSTR is displayed in a white-bordered box. The letters 'W', 'S', and 'R' are white outlines, while the letter 'T' is a solid yellow. The box is connected to a white line with circular nodes on either side.

WSTR

Get the latest on social media and scams, and take a look ahead to the threat landscape of the near future.



ABOUT SYMANTEC

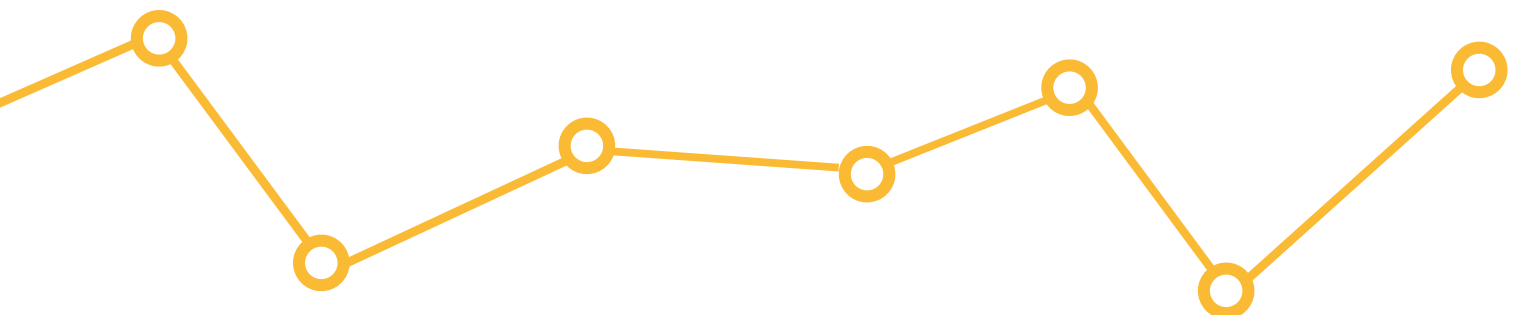
Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of \$6.9 billion.

To learn more go to www.symantec.com

or connect with Symantec at: go.symantec.com/socialmedia.

More Information

- Symantec Worldwide: <http://www.symantec.com/>
- ISTR and Symantec Intelligence Resources: <http://www.symantec.com/threatreport/>
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Norton Cybercrime Index: <http://us.norton.com/cybercrimeindex/>



For specific country offices and contact numbers, please visit our website.

For product information in the US,

Call: 1-866-893-6565

The logo consists of the letters 'WSTR' in a bold, sans-serif font. The 'W', 'S', and 'R' are white with a thin black outline, while the 'T' is solid yellow. The logo is centered within a dark grey rectangular box with a white border. A white line with circular nodes passes behind the box, extending from the left and right edges of the page.

WSTR

Symantec World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

1-866-893-6565

www.symantec.com/ssl

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, the Checkmark Circle Logo, and the Norton Secured Logo are trademarks, or registered trademarks, of Symantec Corporation, or its affiliates, in the U.S. and other countries. Other names may be trademarks of their respective owners.