APRIL 2015
VOL. 17 | NO. 3

INFORMATION SECURITY

Digital Invasion

THE INTERNET OF THINGS AND BYOD CAN TURN INTO A BEACHHEAD FOR ATTACKERS.

TechTarget

Lack of Cybersecurity Awareness Linked to CIOs

Security awareness training remains hit or miss. That may change as calls for accountability from chief executives grow louder.

BY KATHLEEN RICHARDS

WITH ALL THE defenses thrown at information security, most organizations are just a click away from an employee downloading potential malware and undetected viruses. Yet, according to a CompTIA survey of HR professionals, only one-third of U.S. organizations require cybersecurity awareness training for employees. And in more than half of the companies surveyed, it's the CIO or director of IT who decides whether to provide mandatory security training. What exactly is going on?

Spear phishing is suspected as the lynchpin that started the Sony Pictures Entertainment hacking incident—an employee likely opened a targeted email and clicked on a malicious link. The hackers stayed in the movie studio's network undetected for months, according to several reports, including a detailed account in *Vanity Fair*, mapping the infrastructure and preparing to hold the company's data "hostage." The attackers made their presence known in late November with vague demands, and then released humiliating data publicly over several agonizing months in a series of eight information dumps.

Think you're immune to this type of scenario? Not so, warns the SANS Institute's CTO Johannes Ullrich, who heads the Internet Storm Center, in his cover story on emerging cyberthreats. Crypto ransomware, which has proved lucrative for attackers, is likely to target more enterprises in the year ahead.

In addition to preventive strategies like education, security researchers such as White Ops' Chief Scientist Dan Kaminsky are talking about faster detection and response to socially engineered intrusions. Sally Johnson

interviewed Kaminsky for her article on the dynamics of social engineering and found a shift in defense strategies toward data-centric protection mechanisms.

Lack of cybersecurity awareness is becoming less acceptable. In addition to calls for shareholders to hold the top executives accountable for costly data exposures, similar tactics can be employed with third-party vendors. Organizations should require the CEOs of contractors to sign off on all service-level agreements, Rebecca Herold tells Marcus Ranum in a wide-ranging Q&A on data security and privacy best practices. Herold, CEO of the Privacy Professor, has conducted numerous surveys for clients that indicate third-party IT technicians who are responsible for enforcing service-level agreement security measures have no idea what's actually been promised in the respective agreements.

Many enterprises could get away with fewer security staff if they focused on getting the basics right.

While companies continue to throw money at information security, many enterprises could get away with fewer security staff if they focused on getting the basics right. At least that's the view held by John Pescatore, SANS' director of emerging trends, who feels that way even though he works for a global security training and certification institute. Technology journalist Alan Earls interviewed Pescatore, among others, for his in-depth look at cybersecurity hiring trends.

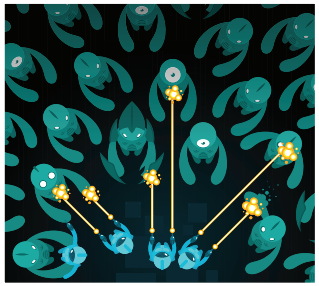
So what's the upshot to all of this? Little to no training and being uninformed are no longer tolerable excuses for vulnerabilities that expose organizations, and the sensitive data they are responsible for protecting, to damaging breaches, even when the security weakness is traced to a third party. As Derek Bok, who twice served as Harvard University president, once said: If you think education is expensive, try ignorance. ■

KATHLEEN RICHARDS *is the* Information Security *magazine features editor. Follow her on Twitter: @RichardsKath.*

DEFENDING AGAINST THE DIGITAL INVASION

The confluence of the Internet of Things and BYOD may turn into a beachhead for attackers.

By Johannes B. Ullrich



IT'S HARD TO forget the recent, and widely publicized, data breaches that upended the fortunes of victimized organizations. Target Corp. attributed $148 million of losses to the breach it suffered. Anthem Insurance Companies Inc. failed to protect millions of healthcare insurance subscribers' Social Security numbers. Sony Pictures Entertainment Inc. has had its internal communications exposed and data wiped off its hard drives. Despite the fallout, in 2015 many security officers will continue to focus on improving the security operations and risk management processes they have in place, with a watchful eye toward business risk and emerging cyberthreats.

Networks are only going to become more complex, increasing the attack surface and moving large parts of the infrastructure outside of corporate control. The confluence of the Internet of Things and bring your own device (BYOD) will start to invade enterprise networks in new ways. Attackers will learn to take advantage of these exposures.

Today little data is lost in most Web defacements. And the attacks, in general, are clearly visible. Security teams

can expect to see more dangerous attacks that are harder to detect in the coming months. Some miscreants may not rely on data exfiltration at all, but instead apply subtle manipulations to data processing systems to influence business decisions.

Up to now, actors using distributed denial-of-service (DDoS) attacks had little reason to innovate. With an ample supply of compromised systems and reflectors available in large numbers to obscure and amplify the attacks, they were able to flood networks with simple requests. However, defensive techniques have improved and anti-DDoS services have become quite capable of stopping all but the largest attacks. DDoS attacks blending in with normal requests that require significant resources to process are much more difficult to block. While cloud-hosted applications may absorb the additional loads, dynamic pricing models could cause significant financial burdens for organizations that come under attack.

We saw criminals perfecting crypto ransomware in 2014. These activities—in which attackers infect systems, encrypt the data and hold it "hostage" until their demands are met—typically targeted consumers and small businesses; this threat has only affected enterprise networks peripherally. But the attackers had significant financial success with these "data kidnapping" methods. The next-generation of crypto ransomware will become more furtive—maintaining business continuity for months after the initial infection takes place. This will ensure that not only current data but also many recent backups are encrypted once the attacker decides to remove the key to ask for the ransom.

When responding to these attack techniques, security teams will have to account for more complex networks. Understanding your infrastructure, defenses and how they are affected by these attack methods is critical in order to provide guidance about your organization's current risk profile.

INVASION OF DIGITAL THINGS

Most chief information security officers have already faced some challenges as traditional workspaces continue to change. For years now, office space has shrunk as more work is being done from employees' homes. But just as work is no longer separated from our personal lives, consumer technology such as wearables and home monitoring systems are invading the enterprise. BYOD was just the beginning.

Consumer-grade devices, which are not included in centralized IT management initiatives, will soon become part of corporate networks. Charging stations for electric cars, fitness monitors included in corporate health plans, devices to monitor and control home security systems, and smart watches will all be connected to corporate networks—like smartphones and tablets before them. But the difference is that these devices will provide even fewer safeguards and far less visibility into their internal

workings. None of these devices will connect to enterprise authentication systems, and the network stack and the number of supported operating systems will be more diverse.

A simple move to replace an old-style television in a break room with a smart TV will expose your network to new threats. This "IT device" will now be connected to your network. At the same time, it will be receiving wireless signals over the air in the form of digital TV transmissions, infrared remote control signals and, maybe, even offering Wi-Fi and Bluetooth connectivity while providing new gateways into your infrastructure. It will not integrate with existing patch management and access control systems.

At this point, we are just starting to understand the threats that we are being exposed to—due to the buggy and incomplete security controls these devices are prone to provide. These devices can easily turn into a beachhead that an attacker can use to compromise your network. Proper onboarding, network segmentation and testing of these devices will be critical, but these processes have to be developed to scale. Policy alone will not protect you in a world where a smartphone contains four or more different radios, and a watch supports at least two.

Just like Target's network was breached via its heating and ventilation system, the next large credit card breach may originate from a smart watch or a smart TV. In 2014, a number of network-connected security cameras were breached giving attackers access to corporate networks. (See: "Device Malware.") Later these cameras were used to scan for network-connected storage devices.

Similar to USB thumb drives of the past, these devices will connect and exchange data with corporate technologies, and potentially introduce malware into our networks, bypassing legacy chokepoint-focused perimeter controls. To detect these threats, controls must be able to monitor lateral movement, and they need to be applied continuously to identify threats quickly. Even if these devices do not have the ability to send and execute files remotely, they may still have access to corporate APIs that can be used to manipulate data and influence business decisions.

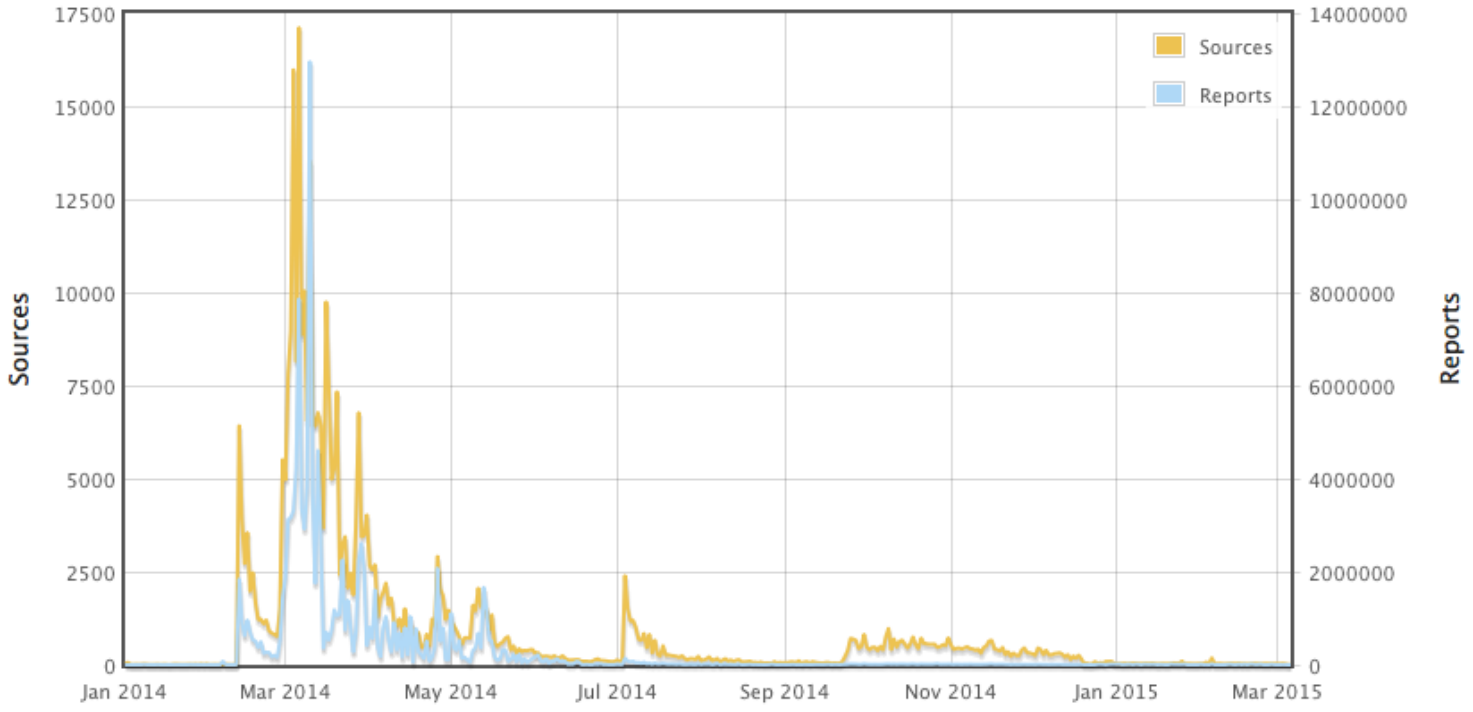
SUBTLE MANIPULATION, HIGH COST

Because untrusted devices can gain access to internal APIs, you are now faced with increasingly subtle and difficult-to-detect attacks. You may still see defaced websites and large leaks of customer data and intellectual property. But in hindsight, you may wish these large, visible threats were all you had to worry about. A defacement of a public-facing website may temporarily damage your company's image, yet it is easily detected and relatively straightforward to resolve. Leaking customer data may require dealing with regulators, and your company may endure significant costs in remediating the breach. Still,

(Continued on page 8)

Device Malware

A SANS Internet Storm Center graph showing the reported attacks against disk storage devices such as digital video recorders on surveillance cameras. The malware scanned for network attached storage devices exposed on port 5000.



SOURCE: SANS INSTITUTE, MARCH 2015

(Continued from page 6)

despite the headlines, most companies still recover, and even thrive, after large data breaches.

That wasn't the case for a CEO whose company was pushed to the brink of bankruptcy after losing a number of high-profile bids to a foreign competitor. Not because its product was worse, but because its price was too high. The price his team quoted was based on a cost estimate derived from an internal enterprise resource planning system. What was the problem? The pricing data was manipulated by malware to provide the wrong results, and the changes were so subtle they were not easily detectable. The outcome was an overstatement of the cost for these projects. No modern business or government today can make decisions without using data analytics, and accurate results are critical. These breaches also escape the public eye because they do not result in the loss of customer information, and the culprits are long gone by the time these breaches are discovered, if they are even detected at all.

DDoS MOBILIZES

Denial-of-service attacks, on the other hand, are easy to spot, but can be difficult and expensive to fight. Over the last few years, we saw the size of DDoS attacks climb significantly. Attackers perfected the ability to collect large numbers of compromised systems and turn them into powerful weapons by amplifying their output using protocols like DNS, SNMP and NTP. While these attacks are powerful and can lead to enormous traffic floods, they can be identified and filtered using specialized anti-DDoS services. Even small to medium-sized businesses are now used to paying thousands of dollars per month for "DDoS insurance."

DDoS attackers may take a step back and target specific application-layer resource bottlenecks, sending fewer but smarter requests that are hard to see.

As a result of better defenses, attacks these days often go unnoticed. And, in particular, large financial companies that were targeted heavily in the past have learned to live with DDoS attacks and experience little disruption as a result. Future DDoS attackers may take a step back and not just flood the network infrastructure. Instead, by targeting specific application-layer resource bottlenecks, attackers may try to send fewer but smarter requests that fit in with normal queries and are harder to filter.

Mobile APIs often do not include sufficient rate limits and are easily exploited to launch DDoS attacks. If the attacks use compromised mobile devices as a launch platform, they are very difficult to distinguish from valid

requests and can easily overwhelm a back-end database. In some cases, it may not even take a full compromise of the device.

Many APIs encourage third-party developers to take advantage of the programming interfaces and, with that, allow and support cross-origin requests from other Web applications. In this case, all it takes is some JavaScript on a popular website to build powerful ad-hoc attack networks that will send requests, which are indistinguishable from valid inquiries.

RANSOMWARE AT WORK

Over the last few years, we have seen crypto ransomware affect consumer, as well as enterprise, desktops. CryptoLocker and similar malware have locked thousands of systems and generated millions in revenue for the miscreants behind it. In the future, we should expect to see more ransomware affecting servers. That includes sophisticated and stealthy varieties that will infect a network for months before divulging that valuable data was encrypted and is no longer accessible unless a large amount of money is paid.

This type of ransomware usually implements a shim between the application and the data store. The data is encrypted and decrypted on the fly, without the application noticing. In some ways, this malware mimics security software that implements database or full disk encryption without disrupting the normal operation of the system. Once the attacker believes enough data is encrypted, the key is removed and the application will fail, asking for a ransom payment to retrieve the key. If the encryption happened for long enough, backups are presumed to be encrypted and unusable as well. The key is often only stored remotely or in memory on the affected system, making it unlikely to be recovered; and even if the malware is detected, it is very possible that the key will not be recovered. With the large financial success gained from desktop crypto ransomware, server-based versions will become more common and even more devastating.

From a defensive point of view, all these threats require a thorough understanding of the network that needs to be protected, consistent controls to enforce security policy and continuous monitoring for compromise. Detecting compromise quickly, understanding the complex interactions between systems correctly to properly contain the compromise and following well-rehearsed incident playbooks is essential. In many ways, it is more important to do what you do now right, instead of looking at new technologies that may further complicate your network defenses. ■

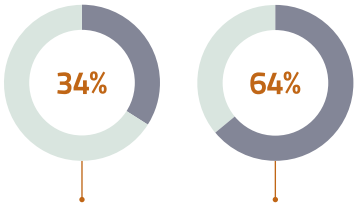
JOHANNES B. ULLRICH, *Ph.D., GIAC, GCIA and GWEB, is chief technology officer at the SANS Technology Institute and head researcher at its Internet Storm Center. Follow him on Twitter: @johullrich.*

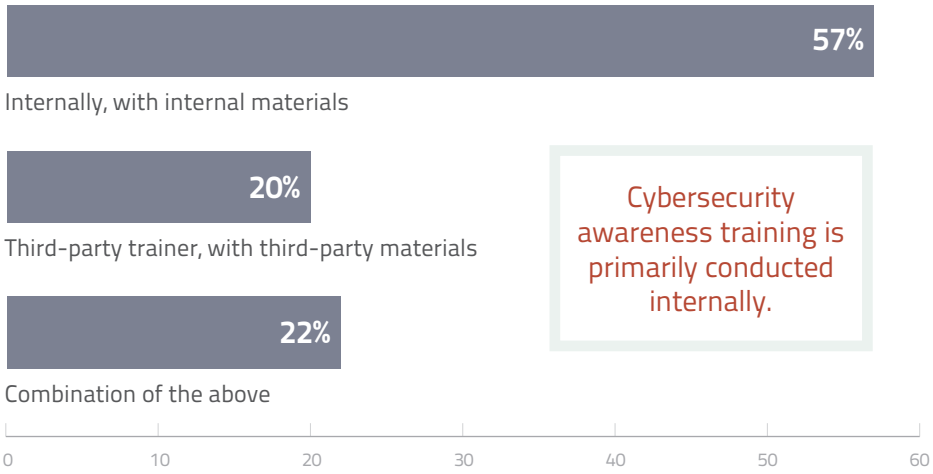
Security Awareness Falls Short

Higher threat levels? No biggie. Cybersecurity awareness training is still not required at two-thirds of the companies surveyed.

Cybersecurity Awareness Training

Only one in three HR professionals report providing cybersecurity awareness training to staff.



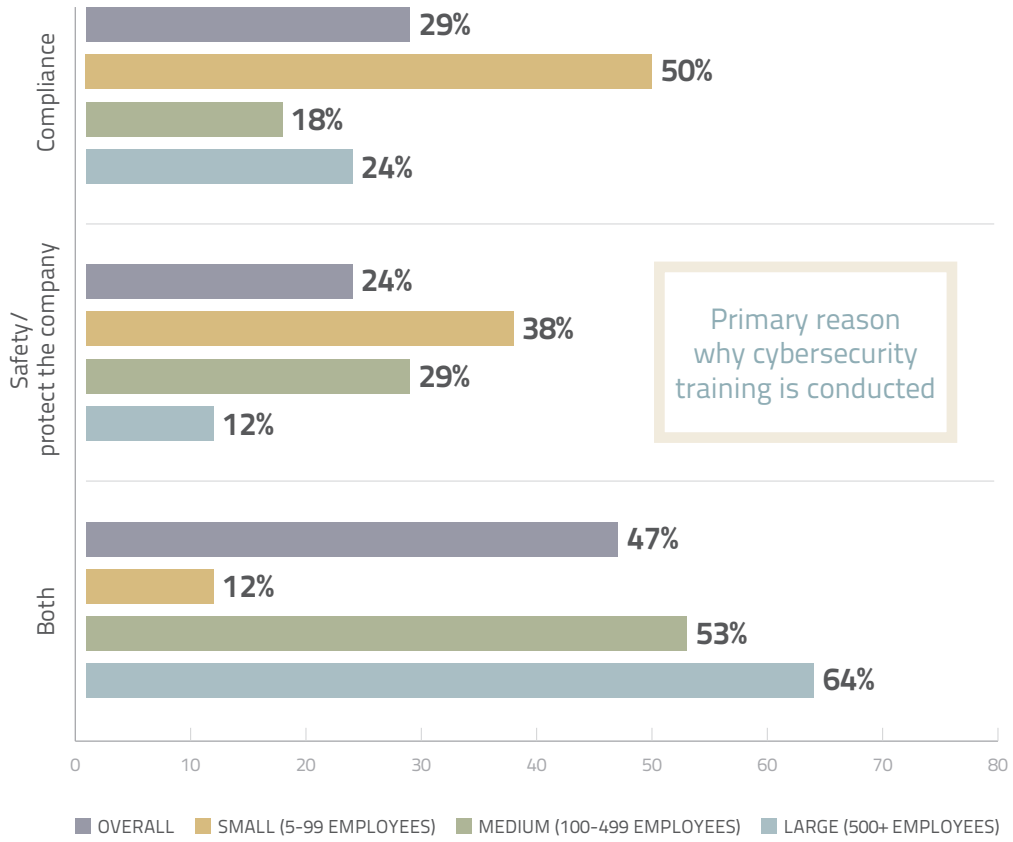


Cybersecurity awareness training is primarily conducted internally.

Small firms (5-99 employees) are more likely to rely on third-party trainers than their larger counterparts.

SOURCE: COMPTIA'S "HR PERCEPTIONS OF IT TRAINING AND CERTIFICATION" STUDY, SEPT. 2014; BASED OFF RESPONSES FROM 400 U.S. HR PROFESSIONALS

Equal Measures: Training Driven by Both Compliance and Safety



Primary reason why cybersecurity training is conducted

Primary decision makers about cybersecurity training

54%
CIO/head of IT

38%
HR

2%
CEO/president

6%
Joint decision among senior leadership

SOURCE: COMPTIA'S "HR PERCEPTIONS OF IT TRAINING AND CERTIFICATION" STUDY, SEPT. 2014; BASED OFF RESPONSES FROM 127 U.S. HR PROFESSIONALS AT FIRMS WITH CYBERSECURITY TRAINING

CYBERSECURITY LABOR PAINS

Why hiring is the next cyberwar.

By Alan R. Earls

THERE IS A hiring crisis in cybersecurity. Many organizations are desperate to find qualified security professionals and fill key staff positions. Consider this from ISACA: According to the 2015 Global Cybersecurity Status Report, which surveyed more than 3,400 ISACA members in January, 92% of those hiring cybersecurity professionals this year say it will be difficult to find skilled candidates. Another 53% of organizations plan to increase cybersecurity training for staff in 2015, while only 9% say they do enough security training already.

"There are currently over a billion dollars worth of unfilled positions globally," says James Arlen, director of risk and advisory services at Leviathan Security Group, a Seattle-based company that provides integrated risk management and information security to Fortune 100 companies and governments.

Companies looking to hire cybersecurity professionals can do themselves a big favor by just simplifying the application process. "Promote employee value and benefits, and put positions in the context of the broader organization," says Jeremy Bergsman, managing director at CEB,

a member-based advisory company based in Arlington, Va. Human resource organizations need to make job postings comprehensible so potential candidates are more inclined to actually apply for open positions.

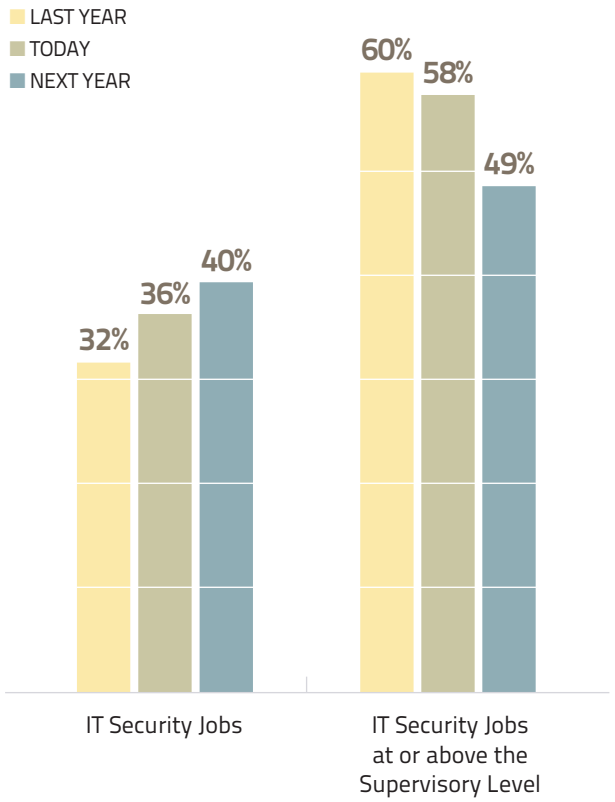
The professional hiring challenge is multifaceted, however. For starters, the breadth of knowledge required for many cybersecurity positions remains a moving target. Job descriptions can ask for expertise across multiple domains—ranging from malware, threat mitigation, cryptography and forensics to industry-specific knowledge, advanced analytics, network virtualization, cloud and mobile security. The failure to find qualified candidates creates an attitude of near panic in some quarters.

The result is skyrocketing salaries, especially after the highly publicized breaches of 2014. While the labor concerns are genuine, experts offer hope beyond the headlines and differing views about the severity of the problem.

IS IT A CRISIS?

Doug Saylors, a director at Information Services Group (ISG), a global outsourcing consultancy in Stamford, Conn., says that up until about four years ago, security was often "buried" within IT, typically supported on a part-time basis by UNIX or Windows administrators. However, as adversaries have grown more capable, companies have rapidly moved to build separate security organizations.

Talent Shortage: IT Security Positions Go Unfilled



SOURCE: "UNDERSTAFFED AND AT RISK: TODAY'S IT SECURITY DEPARTMENT," FEB. 2014 PONEMON INSTITUTE, SPONSORED BY HP ENTERPRISE SECURITY

"This has resulted in increased salaries and a shortage of qualified [staff for] small to medium enterprises in the marketplace," he says. One ISG client lost a five-year employee who "literally doubled his salary for a similar role that was less than five miles" away, according to Saylors—despite an internal HR study, 14 months earlier, that had determined the employee was paid a competitive salary.

John Pescatore, director of emerging security trends at the SANS Institute in Bethesda, Md., agrees that there is a shortage of capable information security specialists. However, beefing up security staff is not always the best strategy for some enterprises.

"Given that my organization is one of the largest training organizations for cybersecurity, it would be natural for me to say we have a skills shortage," he says. "But in a lot of cases this attitude comes from a general belief that the answer to cybersecurity threats is to throw more

U.S. Salaries for Security Staff Expected to Increase

JOB TITLE	2014 SALARY RANGE	2015 SALARY RANGE	PERCENT CHANGE
Chief Security Officer	$126,750 - $189,750	$ 134,250- $204,750	7.1
Data Security Analyst	$100,500 - $137,250	$ 106,250- $149,000	7.4
Systems Security Administrator	$ 95,250 - $131,500	$ 100,000 - $140,250	6.0
Network Security Administrator	$ 95,000 - $130,750	$ 99,250 - $138,500	5.3
Network Security Engineer	$ 99,750 - $131,250	$ 105,000 - $141,500	6.7
Information Systems Security Manager	$115,250 - $160,000	$ 122,250 - $171,250	6.6

SOURCE: "ROBERT HALF 2015 SALARY GUIDE FOR TECHNOLOGY PROFESSIONALS." DOES NOT INCLUDE BONUSES AND OTHER COMPENSATION.

people at the problem."

Before senior management starts hiring information security specialists, they should look at IT processes as well as user education and awareness programs, he advises. "The reason so many enterprises need more security people is because they are doing basic things wrong in IT—not keeping up with patches and misconfiguring things."

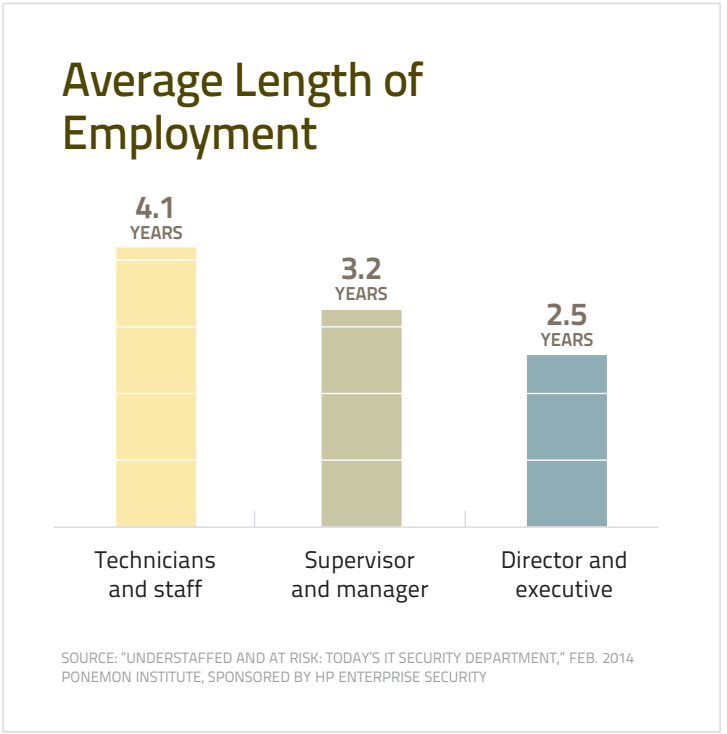
Those initiatives won't solve all the problems. "But if you can reduce major breaches from once a year to, say, once every three years, you can do without a lot of security people," he says.

FINDING TALENT

If more staff is required, a big challenge for most companies is finding the skill sets that they need in specific locations. The cybersecurity talent tends to be clumped in a relatively small number of geographic areas, while the need for cyber skills is widely distributed. The only way to hire right now is to steal people from other organizations. Or import them, Pescatore says.

Leviathan's Arlen, who is Canadian, refers to himself as part of that "brain drain," in which firms pull tech talent from other countries to meet their needs. For American firms, Arlen says, the H1B mechanism can help—but there are strict limits on the number of people that can be brought to the United States and employed with these visas, and there are time restrictions. Another challenge is the citizenship requirement imposed on many government or government-contractor positions.

The North American Free Trade Agreement should offer some help, but NAFTA was developed a generation ago and its specific language has no special provision for cybersecurity. NAFTA also deputizes border patrol people—who have no special expertise—to determine whether an individual seeking to cross the border for



employment is sufficiently qualified. "I had 18 years of experience, including a period in charge of cybersecurity for the Ontario power grid, and I was told at the border that I didn't have the right credentials," Arlen says.

TRAINING AND DEVELOPMENT

Many organizations have underinvested in training, even though more education could enable them to turn good IT or networking staff into security specialists. "The bill for that failure is starting to hit," Pescatore says. There are ways to increase the pool within the United States by training more IT people to become security specialists. That includes looking at untapped sources. Several training organizations are now targeting former military people who have worked in the IT area. "With some mentoring to get into private industry, they can be a nice addition to the talent pool," he says.

Education is another avenue to improving the

STEMing the Tide

GETTING MORE KIDS interested in STEM (science, technology, engineering and math) is often cited as the way to boost the nation's competitiveness and support innovative high tech. However, according to Kevin Kelly, CEO of LGS Innovations, a Herndon, Va., provider of network and communication solutions to governments and businesses, it is especially critical for the U.S. government. "The Department of Defense and companies like LGS Innovations are among the largest employers of cybersecurity professionals and STEM graduates," says Kelly. "One of the challenges being faced in the public sector is not just a shortage of cybersecurity professionals, but a shortage of cyberworkers that can be cleared."

Many government cyberpositions require citizenship for high-level security clearances. There is an immediate need to boost domestic STEM initiatives, according to Kelly, because there will be a shortage of 230,000 qualified advanced-degree STEM graduates by 2018. "As a nation, we need to begin exposing our high-school and middle-school aged children to the technologies germane to the cybersecurity challenges through programs like CyberPatriot to begin building our pipeline of future cyber experts," he says.

In addition, as systems increase in complexity, there will be a growing need for cyberexperts to ensure each component sourced within the global supply chain is free from cybervulnerabilities, Kelly adds.—*A.E.*

cybersecurity workforce. (See: "STEMing the Tide.") But many companies remain dubious about the efficacy of degree programs.

Arlen currently serves on the advisory board for an information security program at a Canadian university. The advisory board is involved in the process of curriculum review, itself the result of a lengthy process. In several weeks, the results will go to the Ministry of Education for approval, a process likely to take many more months. The bottom line is that the curriculum probably won't be implemented until 2017, and graduates will not emerge until 2021 at the earliest, by which time, he notes, much will have changed in the field.

Indeed, says Arlen, IT pros often have to "untrain" recent graduates who learned about the field from books written as much as a decade earlier. However, given the perceived talent shortage, even those with the barest of skills can now command substantial entry-level salaries, even though "degree-less people with a Mohawk and a kilt may be the ones that are actually making the meaningful contributions," he says.

No matter the field, employers almost always complain that the college graduates they hire "don't know anything," Pescatore says. Colleges could improve their results if they relied more on practitioners to teach and if they emphasized more hands-on "lab" work. The key is not getting people to pass quizzes, "it's operational excellence, doing it better than the bad guys," he says.

RAND Considers Cybersecurity Labor Woes

RAND CORPORATION, the famous think tank, published a report in June 2014, "Hackers Wanted: An Examination of the Cybersecurity Market," on behalf of its government clients. It takes a surprisingly measured view of the shortage of cybersecurity professionals. The authors—Martin C. Libicki, David Sentry and Julia Pollack—start with a careful review of factors that contribute to the problem in government as well as the range of potential solutions. However, in the final analysis, they suggest that the panic may be misplaced and that labor market equilibrium could return. The authors draw analogies to the Cold War-era aerospace boom that fueled careers but also left other folks stranded at mid-life when the threat picture changed. Furthermore, they speculate that fundamental changes in computing and IT security could alter the cybersecurity threat picture for the better in coming years. *—A.E.*

WHAT SKILLS MATTER MOST?

When it comes to filling cybersecurity positions there are differing views about formal training and certification versus experience. However, the bottom line is that security professionals need to demonstrate specific skills that may not be as valued in other career paths, says Chris Bucolo, senior manager of partner relations in the security and compliance practice of Sikich LLP in Chicago.

IT people may know about different aspects of security but often lack a broader perspective. Key attributes for career success in cybersecurity include the following:

- Proven ability to think on their feet. Many threats are very fast moving and can pop up out of nowhere.
- Skills to troubleshoot and find the source of problems.
- Able to think critically rather than just watch things unfold.
- A willingness to do things differently and persuade others to try something new. For example, balancing user experience issues with security needs.
- The ability to implement change and help an organization adapt to a new security requirement or challenge.

Fortunately, says Bucolo, there are IT people who can make the leap, especially individuals who can understand the bigger picture. "The technology things matter deeply, but it is still vital to have an ability to relate it to the organization and the people," he says. "That can have a big impact on whether data actually gets lost."

"Many companies are still at an early phase of their efforts to fully secure their systems," says Shawn Panson, leader of PwC's U.S. risk assurance emerging services practice. So, building that needed capability will take time.

A good strategy is to evaluate current employees and consider whether they have the critical-thinking skills necessary to respond to cyberthreats, asserts Bucolo: "We are not doing a good enough job of assessing existing talent and whether some individuals in our organizations might have real aptitude for handling bigger security issues." ■

ALAN R. EARLS *is a freelance journalist based near Boston. He focuses on business and technology, particularly storage, security and the Internet of Things.*

Data Insecurity: Don't Let Third Parties Skate

Organizations will be judged by the company they keep, warns the Privacy Professor CEO. BY MARCUS J. RANUM

IT'S HARD TO ignore the parade of headlines that point to breaches caused by third-party security lapses. Yet organizations still fail to monitor contracted vendors until it's too late.

"Responsibility follows the information," cautions Rebecca Herold, CEO of Privacy Professor and partner at Simbus Security and Privacy Solutions. While third parties come through breaches unscathed, organizations from Target Corp. to Dairy Queen often pay a steep price for public incidents traced to vulnerabilities that vendors introduce.

That doesn't surprise Herold, who has performed audits for companies of all sizes: "I could fill hundreds of pages with the security and privacy incidents that contracted entities have caused," she says. A 25-year veteran who specializes in privacy and compliance, Herold is working on her 17th book, which explains how to establish a third-party security and privacy risk management program.

Marcus Ranum caught up with Herold, who is an adjunct professor for the information security and assurance master of science program at Norwich University Online, to discuss the problem with service level agreements (SLAs), and why a lot more action on the part of senior management is needed.

MARCUS RANUM: I'm really excited to have a chance to ask you a bunch of questions about privacy and working with third parties. It seems to me that the prevailing wisdom is: Get an SLA. Right?

REBECCA HEROLD: It's not really wise. But yes, it has been

the long-standing [practice] of most organizations, often strongly supported by executive management, whose lawyers found ways to say: 'Oh, no, Mr. BigDog; we really don't need to do anything more than get our contracted parties to sign an SLA, along with a hold-harmless agreement.'

Organizations are starting to realize they must do more. Significant numbers of breaches are caused by the contracted entities doing work for their business clients. Look at the large Target breach at the end of 2014; it was caused by a contracted vendor that left the HVAC vulnerable. Do you know what the name of that vendor is? No, but you sure know that it was the Target breach.

It's more complicated than that, though, isn't it?

Responsibility follows the information. The blame in the court of public opinion—and oftentimes, a judicial court—goes to the business that collected the consumers' information.

Look at the privacy breaches that occurred at hundreds of Jimmy John's [locations], Dairy Queens, Chick-fil-As and other restaurants in the summer of 2014. All caused by the same point-of-sale system vendor. Did that vendor's name make the headlines? Did the vendor pay for all the credit monitoring? No. Responsibility follows the data, and, generally, the blame remains with the company that collected the information from the individuals to begin with.

Rebecca Herold

Just this week a New York healthcare provider had the health information of 2,700 patients breached. Did it cause that breach? No, one of its business associates lost a laptop and a smartphone that contained that information. Here's the fun fact: The laptop was encrypted, but the nurse using it had the encryption key in the laptop bag that held the laptop. The smartphone did not have any security on it at all.

The business associate is obligated under HIPAA [the Health Insurance Portability and Accountability Act] to follow all the security and privacy requirements, but she didn't, so she faces penalties. And so could the healthcare provider if the U.S. Department of Health and Human Services' investigation shows it did not take actions to reasonably assure its business associates had appropriate security in place.

I know it's a complicated problem and I'm afraid it's one that gets swept under the carpet.

Yes, it is complicated. But organizations need to realize they must know more about the risks that their contracted vendors are bringing to them, and then establish a security and privacy oversight program for third

parties—contractors and business associates—to effectively deal with it. They have to understand that the businesses they are entrusting with their information, and access to their systems, must have at least the same level of security as [the controls] they require for their own organization. But most do not.

Since 2000, I've done over 300 third-party reviews and audits, including vendor, information security and privacy programs. ... The risks that these small-to-large businesses, in all industries and locations throughout the world, brought to the companies hiring them—and the associated information assets—were often significant. But, in most cases, the companies contracting with them had no clue and the third party also had no clue that what they were doing was putting information assets at huge risk.

Here are just a couple of examples:

A large multi-national financial corporation hired a small—five-person, all family members—business to house the systems for one of its newly acquired business offerings, which had about 80,000 clients. The small business did not have any disaster recovery plan documented: 'We all live together and talk every day, so we know what to do.' [It] only made backups once a month, and it did not have the client data stored on its Web server encrypted. ... My client made sure the vendor improved upon its information security and privacy program, which was pretty much non-existent, in order to continue their contract.

Another client, a large hospital system—a HIPAA-covered entity (CE)—outsourced patient calls about billing. I discovered the business associate wrongly believed anything that could be found publicly—names, addresses, phone numbers and email addresses—was not considered protected health information. They were creating databases with all such data from their CE client and selling it to marketing firms, among many other risky and non-compliance actions; the CE terminated the contract.

In a large number of situations, business associates—and vendors in general—do not have a dedicated position for information security or privacy; or that position is in name only, and the person filling it has no experience or understanding of actually implementing information security or privacy protections. ... I spent the past year creating a new service to help businesses to effectively manage and oversee the information security and privacy risks of their third parties on an ongoing basis, so they can more quickly discover risks and address them right away. I'm focusing on the healthcare space initially, but then this year I will make another such service available for all types of industries.

Executive leadership must open their eyes to the many risks that contracted entities present to their business. Then invest the time and resources into an effective vendor information-security and privacy-oversight management program.

What are some of the pieces of the process that an organization should have in place? I'm assuming it's more of a process and management problem than a technical one, isn't it?

Yes, it really is a management process, but certainly technology can be used to support it. … At a high level, organizations need to identify all their vendors that have access, in some way, to their information—of all forms—and information systems. Most of the organizations I've talked with throughout the years haven't done this. It should be documented.

Identify the risks those vendors present to the organization based on a variety of factors, including the types of information they are accessing, whether or not they are storing sensitive and personal information within their own systems, and the types of safeguards they have in place for those systems. Document it.

Determine which vendors are high, medium and low risk; then dedicate attention appropriately. Perform regular security and privacy reviews—there are many ways to do this—for the high-risk vendors, as well as appropriate checks for the medium- and low-risk vendors. Keep an eye out for any published reports of breaches for the vendors they are using.

Keep including the security and privacy clauses in vendor contracts. And make sure they contain sufficient details of the requirements necessary for the types of services the vendor is providing; also, be sure to include a right-to-audit clause. Based upon the amount of risk the vendor brings with it, the organization may also want to include penetration testing and vulnerability testing within that audit clause.

Terminate the contracts of vendors that will not appropriately mitigate their risks. Yes, I know this can sometimes be challenging to do, based upon the services the vendor is providing and any long-standing contract. However, if they are putting your organization at significant risk, it isn't worth continuing the relationship and contract.

Hearing your suggestions, the first thing that comes to mind is the old Russian proverb 'Doveryai, no proveryai'—Trust, but verify. In the early '90s, I knew a garage startup that was planning to offer a secure mobile email service to the federal government, and their service agreement basically said, 'If something goes horribly wrong, we'll go out of business.' It seems to me that not enough thought goes into how to put the worms back in the can once they've gotten out, or if that's even possible. What do you tell organizations about that?

Indeed, trust but verify! And I'm happy to see you attribute that saying to the Russians and not to Reagan or one of the other politicians more commonly cited.

Yes, SLAs are just words on paper. ... In those 300-plus vendors' reviews I performed, one of my questions to the IT and security managers was whether or not they had implemented all the requirements within the SLAs. In 80% to 85% of the responses, the people responsible for actually implementing the security and privacy controls had never even seen the SLAs.

The SLAs were typically established and signed by the acquisitions or legal areas, and then nothing more than, 'Yep, we've got the legal taken care of ... go to it,' was ever communicated to the IT and information security groups. This was a real eye-opener for the three large entities for which I did the bulk of those audits. … They changed from a purely contract-based process to following a more hands-on, ongoing communications process with their vendors.

And for their high-risk vendors, [they started] requiring the CEOs to submit monthly attestations—the CEO of a business associate with 400,000 employees in India did this, along with other validating documentation, back as early as 2003; I was impressed. Other vendor requirements included undergoing third-party audits at least annually; having the vendor complete an online risk assessment—I have an advanced-capability version of this coming out this quarter; providing a recent, no older than six months, SSAE 16/ISAE3402 SOC 1 Type 2 report that shows satisfactory assurances are in place; and so on. The best assurances to use depend upon the types of risks the vendor brings.

Regarding getting the cats herded once they're loose—to use a cuter, cuddlier idiom—it is possible, if the organization wants to continue doing work with the contracted vendors. And many do if they have established a personal business relationship with those working at the vendor, and know and trust them to make the appropriate changes.

On the other hand, one of the clients that I did over 100 reviews for used the results … to terminate the relationships of vendors that were revealed to have bad security practices. In some of those cases, the executives were looking for a way to terminate the relationship established through a legacy multiyear contract anyway.

A friend of mine who worked for a big Internet service provider once told me: 'We have never made good on an SLA, because our sales guys just tell them, 'We'll give you free service for a month' instead.' Do you recommend a means test for providers?

Those tables were turned by one of my large—200,000 employees—multinational manufacturing clients. They got fed up with the bad service, systems' downtime and various 'little' breaches that they were experiencing from their contracted vendors. So they included in their SLA: 1) For every minute their system was down as a result of the contracted vendor, the vendor would have $5,000

deducted from the next payment from my client; and 2) for every personal record breached as the result of the contracted vendor, the vendor would have to pay for 2 years' credit monitoring for each individual and would have $500 per individual record deducted from the next payment from my client. The CISO there told me the uptime increased dramatically, and the number of breaches fell dramatically. So this worked for them, probably because they were a huge organization that a lot of vendors did outsourced work for and wanted to continue doing work for. For smaller organizations that outsource, this would probably be a harder requirement to get approved.

Right-to-audit seems to me to be one of those things that sounds good on paper but is probably insanely difficult in practice. The results can be terrifying. I have one friend who had a provider that was required by contract to keep its browsers patched and up to date before accessing a certain system—so they looked at the browser identifier strings and found the provider was less than 50% compliant. I'm sure you've seen stuff like that.

Yes, I strongly recommend a right to audit for high-risk vendors and providers. … And you are right; the results of the assessments often were startling and scary for the client that contracted me.

I also check to see if the executives of the vendors have any current lawsuits against them, or felonies, or if the organization itself has been sued. There are multiple examples I could give. But in one case the CEO of a mid-size company was currently being prosecuted, along with his organization, for financial fraud, yet he had answered the question on my initial questionnaire: Have you ever been sued or prosecuted for financial crimes? 'No.' This shows how answering an assessment questionnaire is important, but not the only thing to be done for vendor oversight.

In a different situation I found that the owner of a small business had just been released after serving several years in prison for money laundering. Perhaps he was reformed, but it was something the client was surprised and interested to find out since the owner had told the client he had a spotless record.

Others are seeing the need for these types of assessments and audits as well. Just consider the recent Anthem hack: Now New York's Department of Financial Services plans to perform security assessments on insurance companies in New York, in addition to updating their regulations. … And since we don't really know yet how this 'sophisticated hack' of Anthem occurred, a thorough audit may reveal multiple security weaknesses, including from the vendors that Anthem uses.

The bottom line: Organizations cannot outsource their responsibilities for safeguarding the information that their clients, customers, patients and others have

entrusted to them.

First, laws and regulations establish organizations' responsibilities for outsourced activities; organizations are usually ultimately responsible for the information they collected and promised the associated individuals that they would protect.

Second, the organization's published privacy notices and policies may indirectly obligate it to track the security and privacy activities of all contracted entities. If an organization promises the personal information it collects will be safeguarded, those promises follow the data to whomever it outsources it to.

Organizations will be judged by the company they keep … the businesses they contract. If organizations don't want to become proactive about their oversight of those contracted entities, I have a question for them: Are they ready to pay for the security and privacy sins of their contracted entities? ■

MARCUS J. RANUM, *chief security officer of Tenable Security Inc., is a world-renowned expert on security system design and implementation. He is the inventor of the first commercial bastion host firewall.*

IS MY DATA BEING BREACHED RIGHT NOW?

Combat social engineering by moving beyond prevention to detection.

By Sally Johnson

NO PREVENTION IS 100% effective against the relentless social engineering attacks on enterprises. In 2014 alone, RSA pegs the cost of phishing attacks on global organizations at an astounding $4.5 billion in losses.

So what's a beleaguered enterprise to do? Along with imparting a solid understanding of impersonation, elicitation and phishing—and encouraging and rewarding employees for reporting any suspicious or odd activities—it's critical for security programs to start expanding beyond prevention.

Today enterprises "use a lot of physical security against social engineering and other threats," says John Kindervag, Forrester Research vice president and principal analyst serving security and risk professionals. "If an attacker gets access to an internal network, it's a successful attack—no one monitors the internal network."

One way to strengthen defenses beyond prevention strategies is by adopting data-centric detection approaches. Organizations are using automated detection and behavioral analytics to watch critical information and how it's accessed—when, where, why and by whom.

"All of information security is moving from prevention to detection, mainly because once a prevention system is defeated the attackers are in," says Dan Kaminsky, co-founder and chief scientist of New York security firm White Ops, which specializes in deterministic botnet detection and sophisticated digital fraud prevention.

COMPLEX 'DANCE' OF SOCIAL ENGINEERING

Email phishing campaigns targeting enterprises are easy to pull off, thanks to social media sites such as LinkedIn, which help attackers exploit the fact that employees tend to trust calls or links in emails from "co-workers."

"A social engineer can go get a list of a company's employees and then generate emails pretending to be from one employee to another, with irresistible bait like a video on YouTube," says Tal Klein, vice president of strategy for cloud application security firm Adallom Inc., in Palo Alto, Calif. "They're tying social elements to phishing, which makes it less likely to detect you've been compromised when you click a link."

The cloud is another attack surface for social engineers who are looking to commit fraud. "Social engineering is more significant than any new virus or backdoor you can imagine," Klein says. Adallom focuses on protecting enterprise employees from phishing and cloud account hijacking attacks, as well as protecting data files inside cloud services, by auditing and ensuring the data side is secure and encrypted and has an audit trail attached to it. Individual behavior can be monitored to establish a behavioral standard deviation, in a manner similar to how banks detect fraud, issuing challenges or alerts to users when unusual activity is detected.

Netskope and SkyHigh Networks are also offering services within this realm, although none of the three are using exactly the same techniques.

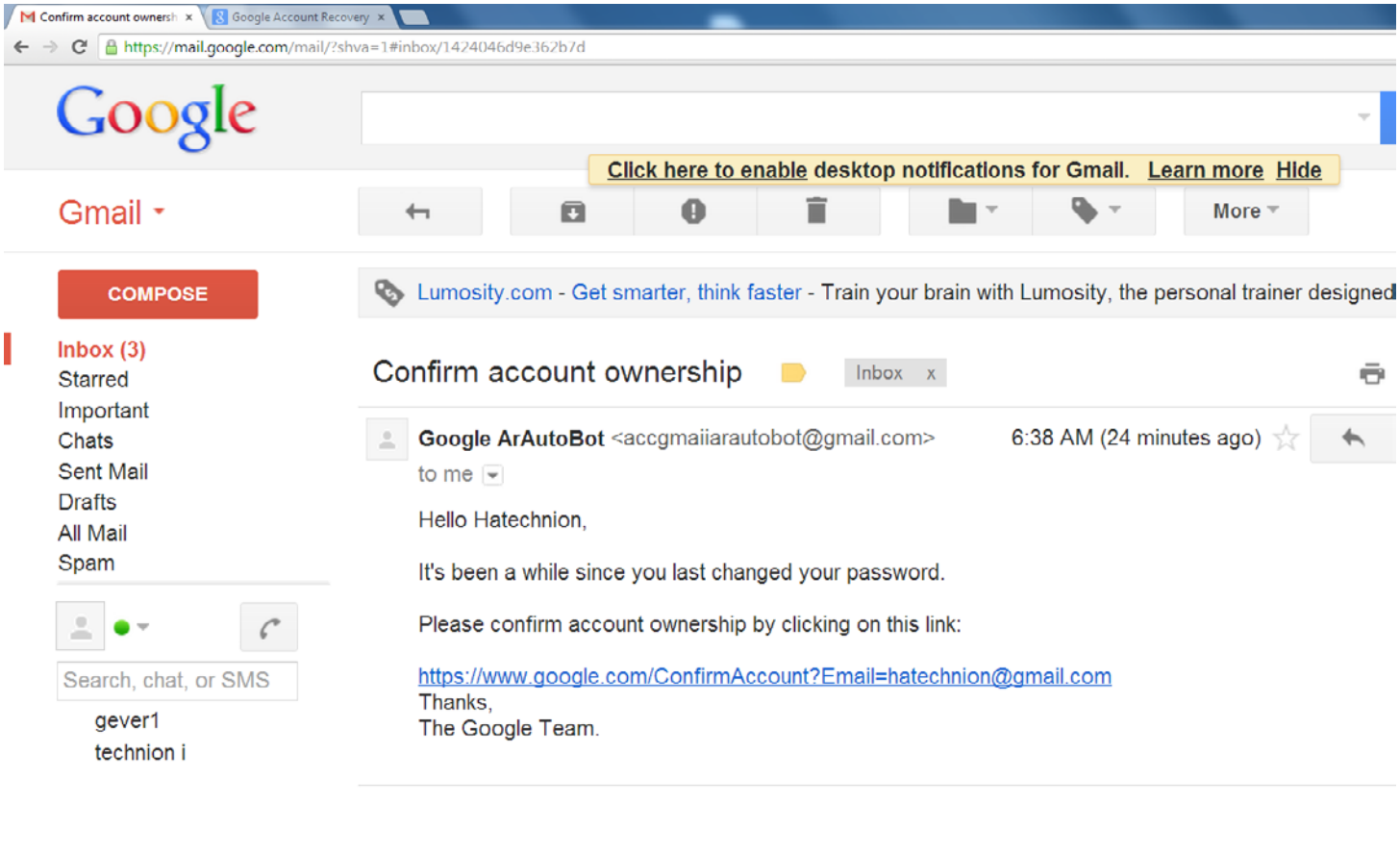
Social engineers are often extraordinarily skilled at tapping into and manipulating relative trust. "Nobody wants to be the person to step on someone else's toes," says Kaminsky, who is well-known within security circles for his research that exposed a DNS caching flaw. "So we're always looking for our role to play, the appropriate thing we're supposed to do based on however we're interacting with someone." And as humans, our default is usually to adopt a cooperative role, which social engineers are all too willing to exploit.

Enterprises are frequently targeted with calls to employees by social engineers—a technique known as pretexting—claiming to be the IT department: "I need your password to fix something of yours." And employees give it up. "Then attackers use these credentials to break in and quickly have their beachhead into the system," he says.

If companies want to lower their risks of becoming victims of social engineering, they need to make employees feel comfortable with slowing down extraordinary

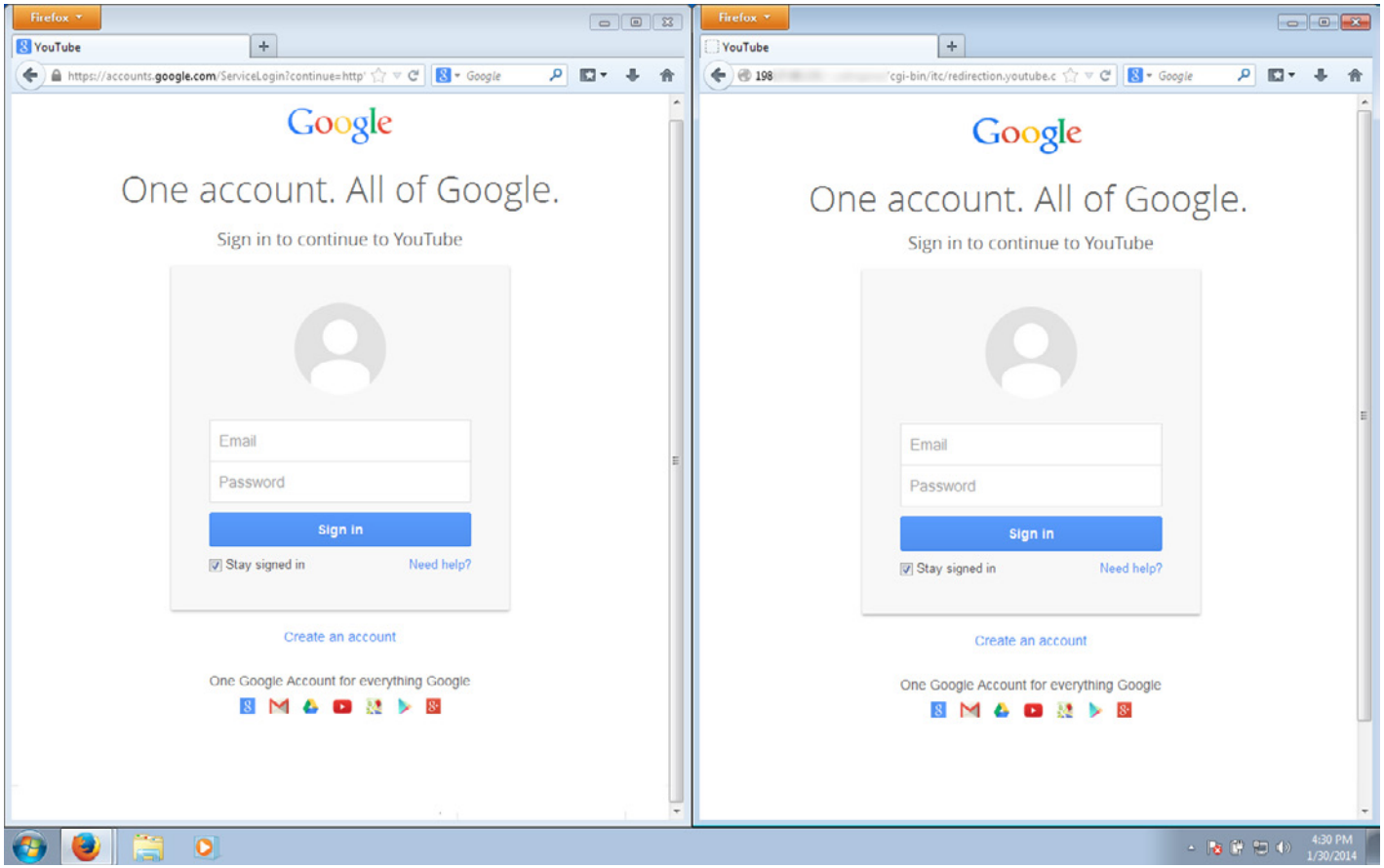
(Continued on page 30)

Phishing email designed to look like it's from Google.



SOURCE: ADALLOM INC.

Same account, but which one is the real Google?



SOURCE: ADALLOM INC.

(Continued from page 27)

requests and validating them. "Make it culturally okay to check," Kaminsky advises. "Take a moment to make sure someone who claims they work for IT actually does. … Say you're going to send them a quick email and make sure they can read it. You're not saying no; you're saying wait a minute. Enterprises need a reporting framework for any weird calls or emails."

Employees should also be encouraged to ask more questions, especially if they think something seems unusual or out of place. "Do we ever stop the UPS person with a package from just walking right into an office?" asks Klein. "No, we always trust the UPS person, or any man or woman in a uniform. We used to do red team data audit tests of data center security, and our goal was to walk into a data center and take our picture right next to our customers' servers. … A janitor uniform makes it extremely easy."

FASTER DETECTION AND RESPONSE

While employee awareness and education can help, enterprises clearly need to do more to stop the malware and other criminal activities that result from social engineering and phishing attacks.

Security vendors are rolling out breach detection systems designed to improve incident response times to help organizations keep pace with attackers. The technologies monitor network communications and use behavioral analytics to help security teams recognize and respond to potential threats.

Several of these vendors are striving to have their systems become big data analytics engines by providing the confidence to allow automation of the breach response.

> **The real secret to protecting data is by adopting a data-centric approach, which relies on securing sensitive data through encryption and other means.**

Some of the companies and products in this group include BAE Systems' Applied Intelligence, CSG International, Damballa, IBM's Q1 Labs, Intel/McAfee's Nitro, LogRhythm and RSA Security Analytics. "If we don't automate, we'll never be able to respond to breaches fast enough," says Kindervag.

"Forward-leaning CISOs and IT security teams are realizing the need to invest in the ability to detect and respond to attacks getting through—that's where automated breach detection systems can provide a platform that enables IT to detect and respond to attacks quickly," says Brian Foster, CTO at Damballa Inc., in Atlanta. Automated breach detection systems can alert you to an infection that can lead to a breach—within seconds and

minutes of it occurring, rather than months afterward.

Damballa's system, for example, analyzes inbound/outbound Internet traffic and doesn't need to sit in the email stream per se, which is where most social engineering occurs through phishing. When the company studied customers' data and the initial installment of malware over a six-month period, it discovered that 20% of files downloaded were from people clicking on malicious email links or inadvertently logging into bad websites. "So one in five was the direct result of social engineering," Foster says.

Some of these technologies may ease the load for security teams. "We simply do not have the resources to identify, contain and remediate malicious attacks on our systems," says an IT specialist for a Global 500 energy and utilities company that uses Damballa's technology. "It has been key in identifying and containing those attacks until they can be remediated. And its custom threat module has finally allowed us to respond effectively to phishing attacks."

ATTACKERS WANT DATA

The real secret to protecting data against theft is by adopting a data-centric approach, which relies on securing sensitive data through encryption and other means. "This tends to protect against risks that are electronic digital hacking versus physical risks of someone social engineering their way into your data center and stealing backup tapes," Kindervag says.

A data-centric strategy is also conducive to big data environments, because it doesn't rely on perimeters to contain the data.

The data-driven security process hinges on getting to know your enterprise assets and classifying the data. "CISOs and CIOs need to identify what their key data is—such as intellectual property—and the IT systems that support it, as well as any risks to the data and systems," explains Foster. "Once you understand this, simple calculations help to figure out how to mitigate the risks … and the costs involved. Then you go invest where it makes sense."

While data classification is no small task, expensive breach cleanups and damaged reputations can be more costly than making the effort to mitigate risks.

"This whole digital life of ours is less than a century old, so it's difficult to think about our digital assets as being physical assets," says Adallom's Klein. "An incremental change in contextual awareness would make a hacker or social engineer's job much more difficult. We need to treat our digital life with the same scrutiny we treat our physical life."

Cloud service providers "do a great job of securing their infrastructure, which was proven time and time again in the breaches of last year," he says. "But none of our existing enterprise controls are effective at protecting data inside the cloud." Firewalls, antivirus and intrusion

prevention systems just aren't effective when users are interacting with data in the cloud from unmanaged devices over public networks. "Putting your data in cloud services like Box, Google Drive or Cloud 365 is actually a lot more secure than on-premises data storage," he adds.

Expect to see more companies come out of stealth mode with automated breach detection offerings in 2015. "This will be a huge cultural shift in the security world, which is very concerned with change," Kindervag points out. "But attackers aren't constrained by the same things that we are, so we need to become much more agile to win this battle."

THE BIG THREE

Earlier detection strategies may help organizations that have relied on prevention approaches, which are clearly not effective. However, the three biggest problems in security have helped to create a perfect storm for social engineering. "We can't authenticate, we can't write secure code, and we can't bust the bad guys," says Kaminsky. "It's not absolutely impossible, but … we can't do any of the three in a way that will scale. And all three of these problems translate to social engineering."

The biggest factor fueling social engineering today is "a lack of consequences for the criminals," he adds. If you can't punish the violator of social rules, society will punish the victim, because they want to establish that

> **"We can't authenticate, we can't write secure code, and we can't bust the bad guys…"**
>
> *Dan Kaminsky, White Ops co-founder and chief scientist*

the victim is unique in some way: That's why they got hit and we didn't. "No one talks about this, but everyone knows it," Kaminsky says. Be sure this doesn't happen to employees reporting social engineering; reward them instead. ■

SALLY JOHNSON *is a freelance technology and science journalist. Previously, she was the features writer for TechTarget's Networking Media and Security Media Groups.*

Big Data Security Gets Serious with NSA's Accumulo and Sqrrl

Competition for Hadoop-based analytics may put tools and services within reach for large and midsize organizations.

BY ROBERT RICHARDSON

NOW THAT THE big data storm has subsided, it's time to move beyond the hype and really look at how machine data might provide actual value to enterprise security. One company that's worth watching is Sqrrl Data Inc. The big data analytics provider announced in February that its Sqrrl Enterprise 2.0 offers "a full-stack security analytics solution for detecting and responding to advanced cybersecurity threats."

The company, headquartered in Cambridge, Mass., entered the market two years ago with a souped-up analysis tool that sits atop a Hadoop installation. The open source framework, hosted by the Apache Foundation, enables large organizations to build a distributed file system across server farms and quickly process searches and queries (programmatically) against large data sets. Enterprise-level analysis tools have been sorely lacking: Now Sqrrl is essentially doubling down on security as a space where a link analysis approach to data yields particularly fruitful results.

The founders of Sqrrl are ex-NSA data crunchers, part of a recent diaspora that has yielded several startups, including Area 1 Security, Synack and Morta Security, which was acquired by Palo Alto Networks in January. In this case, key founders of Sqrrl were involved in the development of Accumulo, a distributed key/value data store designed to handle the huge amounts of data sorted and sniffed by that ever-curious intelligence entity in Fort Meade. Roughly speaking, all those metadata-snarfing, top-secret programs that NSA whistleblower Edward Snowden exposed used Accumulo as their repository. The

NSA released Accumulo as an Apache open-source project in 2011.

Accumulo's roots were in Google's BigTable project, which was highly influential in producing the current buildout of NoSQL databases. Among databases of its particular flavor of NoSQL (wide-columnar), Accumulo is the third-most deployed, after Cassandra and HBase. Accumulo uses a Hadoop distributed file system, which enables the processing of enormous data sets. Because three copies of the dataset are stored, an entry-level Hadoop cluster is often comprised of three standard Linux servers storing up to 10 TB each. If you've got more than 10 TB of data, you add servers.

The inherent advantage of a wide-columnar store is that it can handle a lot more data a lot faster than the relational databases found in security information and event management (SIEM) deployments. "Traditional SIEM systems have had a hard time keeping more than 30 or 60 or maybe even 90 days' worth of data, because all these systems were developed in pre-Hadoop days," said Ely Kahn, Sqrrl's vice president for business development. "But we can take petabytes of data and not only store it cost-effectively but also search and query it at near real-time speeds."

Fortune 20 companies are "literally looking at trillions of unique nodes," Kahn said. Although Sqrrl's software knows how to look for anomalies, he added, it also allows security analysts to be more efficient with their time, which is probably more important.

The approach Sqrrl takes in organizing and processing a year's worth of all kinds of machine and network log data is based on visualizations of the links—or associations—between elements. "Google is probably the purveyor of the most popular graph algorithm in the world," Kahn noted, "which is, of course, called PageRank. A lot of the way that Google does its searches on its semi-structured data is using graph algorithms that look at the links between Web pages to determine the importance [rank] of Web pages."

Right now, it's primarily the largest enterprises whose security analysts can take advantage of Sqrrl and link analysis. But Sqrrl isn't the only game in town—both Palentir Technologies Inc. and RSA offer Hadoop-based analytics of one kind or another, and it seems possible that competition may drive pricing down to levels more palatable for midsize organizations. The Securities and Exchange Commission hired Palentir in 2014 to help it detect insider trading through data analysis of investors' transactions prior to mergers and acquisitions and other deals related to public companies. In the meantime, if you want to bring spy agency technology to bear on your attackers and you've got a global enterprise reach, you'll want to give these tools a look. ■

ROBERT RICHARDSON, *is the editorial director of TechTarget's Security Media Group. Follow him on Twitter: @cryptorobert.*

TechTarget

TechTarget Security Media Group

EDITORIAL DIRECTOR **Robert Richardson**

FEATURES EDITOR **Kathleen Richards**

EXECUTIVE MANAGING EDITOR **Kara Gattine**

ASSOCIATE MANAGING EDITOR **Brenda L. Horrigan**

EXECUTIVE EDITOR **Eric Parizo**

SITE EDITOR **Robert Wright**

DIRECTOR OF ONLINE DESIGN **Linda Koury**

COLUMNISTS **Marcus Ranum, Pete Lindstrom**

CONTRIBUTING EDITORS **Kevin Beaver, Crystal Bedell, Mike Chapple, Michele Chubirka, Michael Cobb, Scott Crawford, Peter Giannoulis, Francoise Gilbert, Joseph Granneman, Ernest N. Hayden, David Jacobs, Nick Lewis, Kevin McDonald, Sandra Kay Miller, Ed Moyle, Lisa Phifer, Ben Rothke, Mike Rothman, Karen Scarfone, Dave Shackleford, Joel Snyder, Steven Weil, Ravila Helen White, Lenny Zeltser**

EDITORIAL BOARD

Phil Agcaoili, Cox Communications
Seth Bromberger, Energy Sector Consortium
Mike Chapple, Notre Dame
Brian Engle, Health and Human Services Commission, Texas
Mike Hamilton, MK Hamilton and Associates
Chris Ipsen, State of Nevada
Nick Lewis, Saint Louis University
Rich Mogull, Securosis
Tony Spinelli, Equifax
Matthew Todd, Financial Engines
MacDonnell Ulsch, PwC U.S.

VICE PRESIDENT/GROUP PUBLISHER **Doug Olender**
dolender@techtarget.com

Stay connected! Follow @SearchSecurity today.

TechTarget
275 Grove Street,
Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

COVER IMAGE AND PAGE 4: RYCCIO/ISTOCK