COLLEGE OF LABOR AND EMPLOYMENT LAWYERS
11TH CIRCUIT REGIONAL COMMITTEE

6TH ANNUAL PROGRAM

Coral Gables, Jan. 21, 2017

# CYBERSECURITY BREACHES and the EMPLOYER'S LIABILITY

## SCOTT A. KAMBER

## KAMBERLAW

*Employers face ever-growing liabilities from sophisticated threat actors, vulnerable enterprise systems, and exploitable employees and their personal devices. Protections and responses involving technology, compliance, insurance, and corporate culture are still immature and rapidly changing.*

*Scott A. Kamber of KamberLaw litigates some of the most compelling technology issues facing corporate America today and will share his views and some strategies.*

**Scott A. Kamber** is the founding member of KamberLaw, the leading plaintiffs' firm to focus on individual rights in the digital age. Serving a global client base with lawyers across the United States, Mr. Kamber has led the successful resolution of dozens of high-impact litigations, including *In re Blue Buffalo*, *Lane v. Facebook*, and *In Re Quantcast* and *Clearspring* ("Flash cookie" litigation). Currently, Mr. Kamber leads numerous litigations arising from various web technologies, wrongful use of deep-packet inspection technologies, web-centric violations of Lanham Act, and website accessibility and the rights of children on the internet. Mr. Kamber has extensive courtroom experience and tried over 15 cases to verdict.

Mr. Kamber's efforts in Internet privacy rights began in the 1990s when he resolved what is believed to be the first Internet privacy case to recover a benefit for impacted class members. His interest in consumer rights and technology extends to new media, and he has led standard-setting litigations and resolutions involving digital rights management software for computer software, video games, and music. Mr. Kamber is a frequent speaker on these issues in the United States and abroad. He was a keynote speaker for the IAPP annual conference and a panelist at the International Conference of Data Protection and Privacy Commissioners, where he spoke on the topic of coordinating private class actions with government enforcement.

Mr. Kamber graduated *cum laude* from the University of California Hastings College of the Law in 1991 where he was *Order of the Coif*, Articles Editor for the *Hastings Constitutional Law Quarterly* and a member of the Moot Court Board. He graduated with University and Departmental Honors from The Johns Hopkins University in 1986. He is admitted to practice before the United States Supreme Court, the State of New York, and the District of Columbia, as well as the United States Courts of Appeals for the Second, Eighth, Ninth Circuits, and several United States District Courts.

# Selected Resources

1. "Online Cheating Site AshleyMadison Hacked," *Krebs on Security*, July 19, 2015, http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/

2. "Attackers Target Both Large and Small Businesses," Symantec, 2016 (*Internet Security Threat Report* infographic), https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf

3. [excerpt] "Managing Insider Risk through Training & Culture," Ponemon Institute Research Report, May 2016 (excerpt), http://www.experian.com/assets/data-breach/white-papers/experian-2016-ponemon-insider-risk-report.pdf

4. "Amid Yahoo hacks, a churn of security officers," Wendy Lee, *San Francisco Chronicle*, Dec. 22, 2016, http://www.sfchronicle.com/business/article/Amid-Yahoo-hacks-a-churn-of-security-officers-10814525.php

5. [excerpt] "Understaffed and at Risk: Today's IT Security Department," Ponemon Institute Research Report, Feb. 2014, http://www.ponemon.org/local/upload/file/IT%20Security%20Jobs%20Research%20Report%20FINAL4.pdf

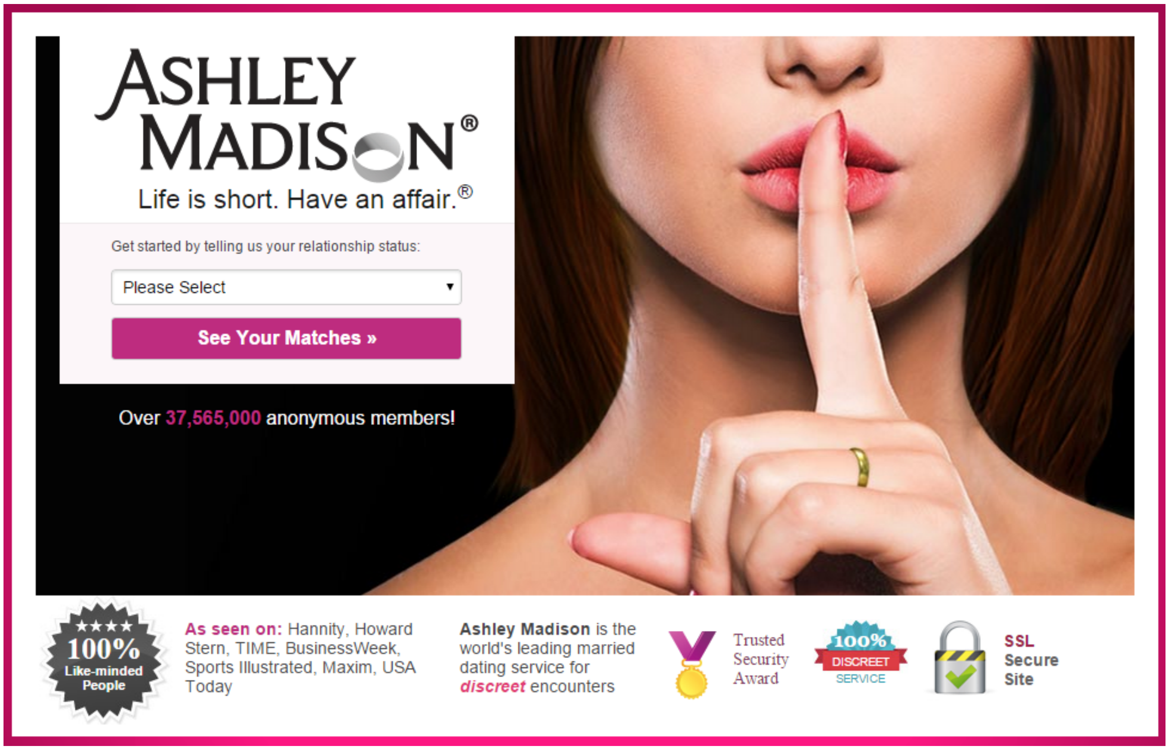
6. "Mitigating the Cybersecurity Skills Shortage," Cisco, 2015, http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

7. [excerpt] "The Defender's Dilemma: Charting a Course Toward Cybersecurity," Martin C. Libicki, Lillian Ablon, and Tim Webb, Rand Corporation, 2015 (excerpt), http://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1024/RAND_RR1024.pdf

# 19 Online Cheating Site AshleyMadison Hacked

JUL 15

Large caches of data stolen from online cheating site **AshleyMadison.com** have been posted online by an individual or group that claims to have completely compromised the company's user databases, financial records and other proprietary information. The still-unfolding leak could be quite damaging to some 37 million users of the hookup service, whose slogan is "Life is short. Have an affair."



Get started by telling us your relationship status:

Over 37,565,000 anonymous members!

As seen on: Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

Ashley Madison is the world's leading married dating service for *discreet* encounters

The data released by the hacker or hackers — which self-identify as **The Impact Team** — includes sensitive internal data stolen from Avid Life Media (ALM), the Toronto-based firm that owns AshleyMadison as well as related hookup sites **Cougar Life** and **Established Men**.

Reached by KrebsOnSecurity late Sunday evening, **ALM Chief Executive Noel Biderman** confirmed the hack, and said the company was "working diligently and feverishly" to take down ALM's intellectual property. Indeed, in the short span of 30 minutes between that brief interview and the publication of this story, several of the Impact Team's Web links were no longer responding.

"We're not denying this happened," Biderman said. "Like us or not, this is still a criminal act."

Besides snippets of account data apparently sampled at random from among some 40 million users across ALM's trio of properties, the hackers leaked maps of internal company servers, employee network account information, company bank account data and salary information.

The compromise comes less than two months after intruders stole and leaked online user data on millions of accounts from hookup site **AdultFriendFinder**.

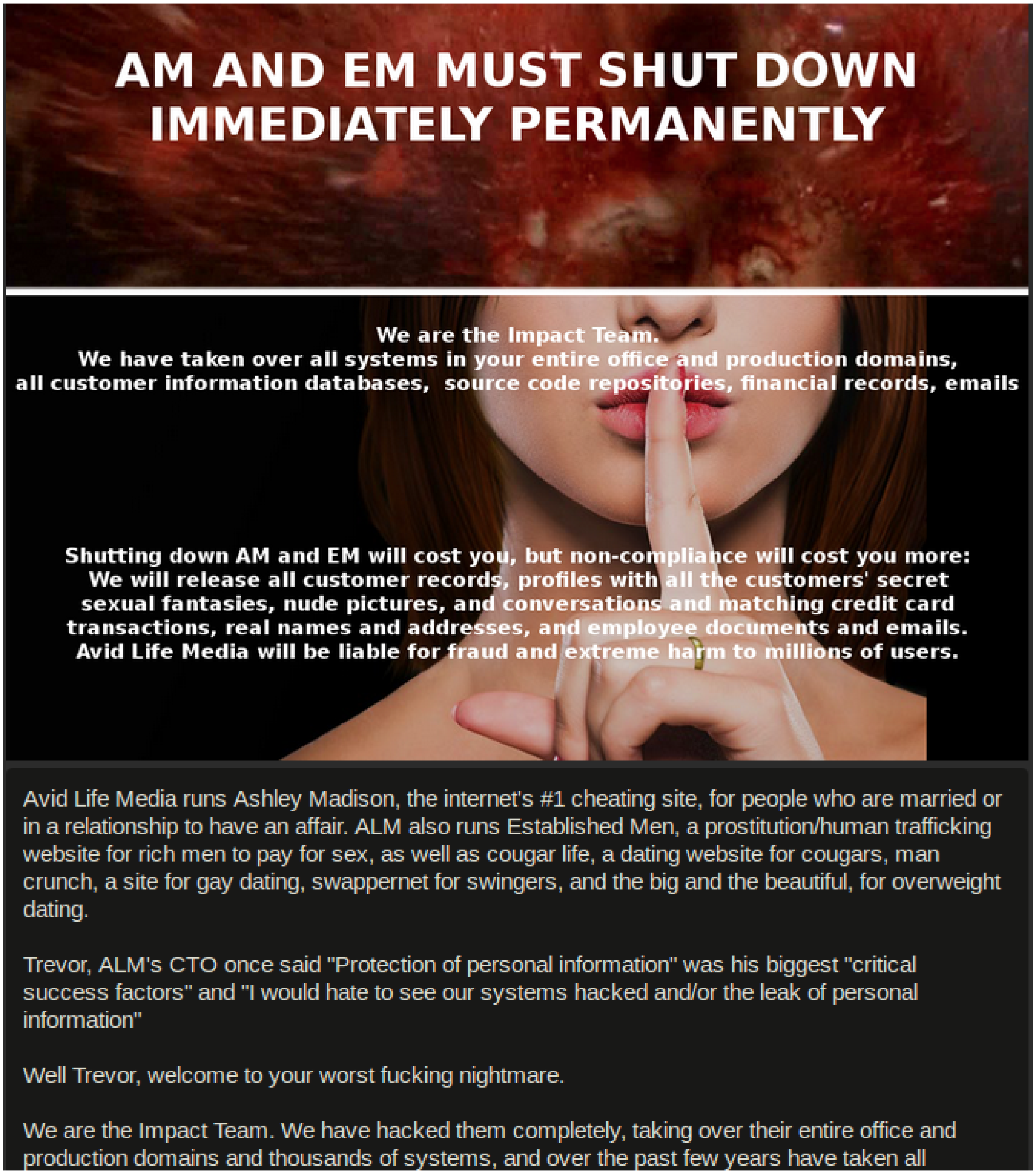
In a long manifesto posted alongside the stolen ALM data, The Impact Team said it decided to publish the information in response to alleged lies ALM told its customers about a service that allows members to completely erase their profile information for a $19 fee.

According to the hackers, although the "full delete" feature that Ashley Madison advertises promises "removal of site usage history and personally identifiable information from the site," users' purchase details — including real name and address — aren't actually scrubbed.

"Full Delete netted ALM $1.7mm in revenue in 2014. It's also a complete lie," the hacking group wrote. "Users almost always pay with credit card; their purchase details are not removed as promised, and include real name and address, which is of course the most important information the users want removed."

Their demands continue:

"Avid Life Media has been instructed to take Ashley Madison and Established Men offline permanently in all forms, or we will release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails. The other websites may stay online."



AM AND EM MUST SHUT DOWN
IMMEDIATELY PERMANENTLY

We are the Impact Team.
We have taken over all systems in your entire office and production domains,
all customer information databases, source code repositories, financial records, emails

Shutting down AM and EM will cost you, but non-compliance will cost you more:
We will release all customer records, profiles with all the customers' secret sexual fantasies, nude pictures, and conversations and matching credit card transactions, real names and addresses, and employee documents and emails.
Avid Life Media will be liable for fraud and extreme harm to millions of users.

Avid Life Media runs Ashley Madison, the internet's #1 cheating site, for people who are married or in a relationship to have an affair. ALM also runs Established Men, a prostitution/human trafficking website for rich men to pay for sex, as well as cougar life, a dating website for cougars, man crunch, a site for gay dating, swappernet for swingers, and the big and the beautiful, for overweight dating.

Trevor, ALM's CTO once said "Protection of personal information" was his biggest "critical success factors" and "I would hate to see our systems hacked and/or the leak of personal information"

Well Trevor, welcome to your worst fucking nightmare.

We are the Impact Team. We have hacked them completely, taking over their entire office and production domains and thousands of systems, and over the past few years have taken all

*A snippet of the message left behind by the Impact Team.*

It’s unclear how much of the AshleyMadison user account data has been posted online. For now, it appears the hackers have published a relatively small percentage of AshleyMadison user account data and are planning to publish more for each day the company stays online.

“Too bad for those men, they’re cheating dirtbags and deserve no such discretion,” the hackers continued. “Too bad for ALM, you promised secrecy but didn’t deliver. We’ve got the complete set of profiles in our DB dumps, and we’ll release them soon if Ashley Madison stays online. And with over 37 million members, mostly from the US and Canada, a significant percentage of the population is about to have a very bad day, including many rich and powerful people.”

ALM CEO Biderman declined to discuss specifics of the company's investigation, which he characterized as ongoing and fast-moving. But he did suggest that the incident may have been the work of someone who at least at one time had legitimate, inside access to the company's networks — perhaps a former employee or contractor.

"We're on the doorstep of [confirming] who we believe is the culprit, and unfortunately that may have triggered this mass publication," Biderman said. "I've got their profile right in front of me, all their work credentials. It was definitely a person here that was not an employee but certainly had touched our technical services."

As if to support this theory, the message left behind by the attackers gives something of a shout out to ALM's director of security.

"Our one apology is to Mark Steele (Director of Security)," the manifesto reads. "You did everything you could, but nothing you could have done could have stopped this."

Several of the leaked internal documents indicate ALM was hyper aware of the risks of a data breach. In a Microsoft Excel document that apparently served as a questionnaire for employees about challenges and risks facing the company, employees were asked "In what area would you hate to see something go wrong?"

**Trevor Stokes**, ALM's chief technology officer, put his worst fears on the table: "Security," he wrote. "I would hate to see our systems hacked and/or the leak of personal information."

In the wake of the AdultFriendFinder breach, many wondered whether AshleyMadison would be next. As the Wall Street Journal noted in a May 2015 brief titled "Risky Business for AshleyMadison.com," the company had voiced plans for an initial public offering in London later this year with the hope of raising as much as $200 million.

"Given the breach at AdultFriendFinder, investors will have to think of hack attacks as a risk factor," the WSJ wrote. "And given its business's reliance on confidentiality, prospective AshleyMadison investors should hope it has sufficiently, er, girded its loins."

**Update, 8:58 a.m. ET:** ALM has released the following statement about this attack:

> "We were recently made aware of an attempt by an unauthorized party to gain access to our systems. We immediately launched a thorough investigation utilizing leading forensics experts and other security professionals to determine the origin, nature, and scope of this incident."
>
> "We apologize for this unprovoked and criminal intrusion into our customers' information. The current business world has proven to be one in which no company's online assets are safe from cyber-vandalism, with Avid Life Media being only the latest among many companies to have been attacked, despite investing in the latest privacy and security technologies."
>
> "We have always had the confidentiality of our customers' information foremost in our minds, and have had stringent security measures in place, including working with leading IT vendors from around the world. As other companies have experienced, these security measures have unfortunately not prevented this attack to our system."

"At this time, we have been able to secure our sites, and close the unauthorized access points. We are working with law enforcement agencies, which are investigating this criminal act. Any and all parties responsible for this act of cyber–terrorism will be held responsible."

"Avid Life Media has the utmost confidence in its business, and with the support of leading experts in IT security, including Joel Eriksson, CTO, Cycura, we will continue to be a leader in the services we provide. "I have worked with leading companies around the world to secure their businesses. I have no doubt, based on the work I and my company are doing, Avid Life Media will continue to be a strong, secure business," Eriksson said."

# Attackers Target Both Large and Small Businesses

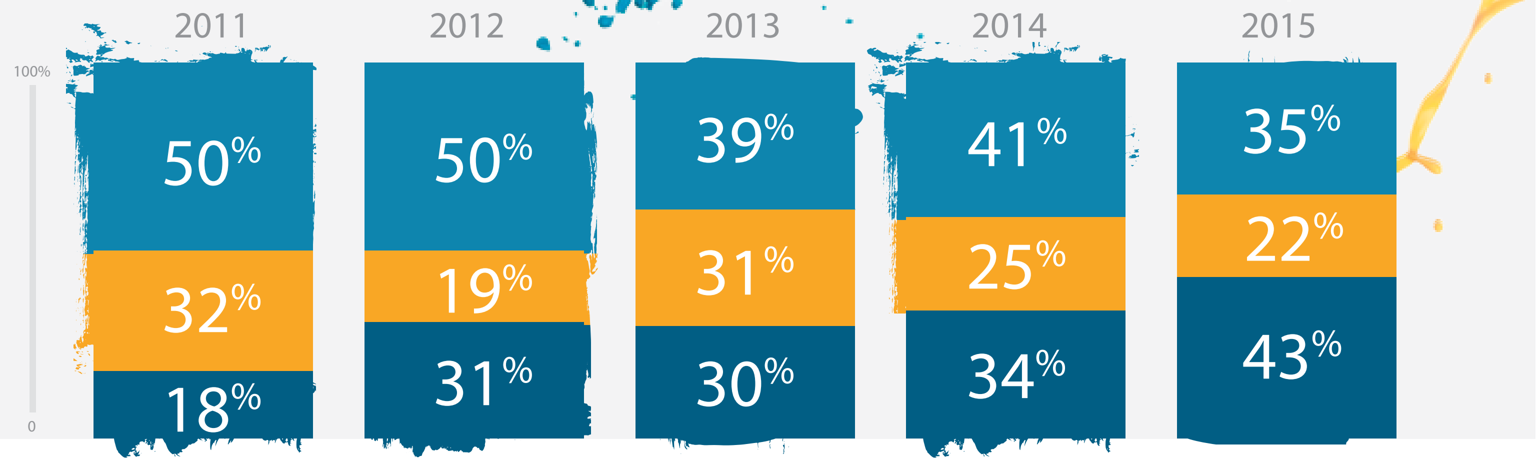
Like thrown paint on a blank canvas, attacks against businesses, both large and small, appear indiscriminate.
If there is profit to be made, attackers strike at will.

The last five years have shown a steady increase in attacks targeting businesses with less than 250 employees.

Number of Employees

- ■ Large Enterprises 2,500+
- ■ Medium-Size Businesses 251 to 2,500
- ■ Small Businesses (SMBs) 1 to 250

Spear-Phishing Attacks by Size of Targeted Organization



Cyber attackers are playing the long game against large companies, but all businesses of all sizes are vulnerable to targeted attacks. In fact, the number of spear-phishing campaigns targeting employees increased 55% in 2015.

| 2013 | 2014 | 2015 |
|---|---|---|
| 779 | 841 | 1,305 |
| +91% | +8% | +55% |

## 2015 Risk Ratio of Spear-Phishing Attacks by Organization Size

| | | | |
|---|---|---|---|
| Attacks per Org | 3.6 | 2.2 | 2.1 |
| Risk Ratio as % | 38% | 15% | 3% |
| Risk Ratio | 1 in 2.7 | 1 in 6.8 | 1 in 40.5 |

Symantec.

# Managing Insider Risk through Training & Culture

## Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC

Publication Date: May 2016

# Managing Insider Risk through Training & Culture

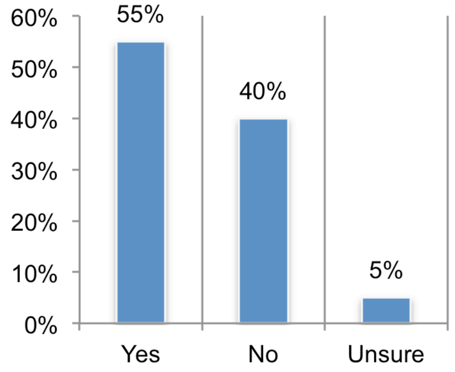
Ponemon Institute, May 2016

## Part 1. Executive summary

Employees and other insiders inadvertently exposing sensitive or confidential information is a nightmare scenario for companies. *Managing Insider Risk through Training & Culture,* sponsored by Experian® Data Breach Resolution, reveals why this security risk persists, despite millions of dollars spent on investments in employee training and other efforts to reduce careless behavior in the handling of sensitive and confidential information. Ponemon Institute surveyed 601 individuals in companies that have a data protection and privacy training (DPPT) program and who are knowledgeable about the program.

### Companies understand the risk

**Figure 1. Did your organization have a security incident or data breach due to a malicious or negligent employee?**



Sixty-six percent of respondents admit employees are the weakest link in their efforts to create a strong security posture. As shown in Figure 1, 55 percent of respondents say their organization had a security incident or data breach due to a malicious or negligent employee.

The top two insider risks, according to respondents, are a data breach caused by a careless or negligent employee who exposes sensitive information or succumbs to a targeted phishing attack. Companies also understand that security risks involve behaviors that could lead to a data breach or other security incident. These concerns are:

- Unleashing malware from an insecure website or mobile device
- Succumbing to targeted phishing attacks
- Using unapproved cloud or mobile applications to send sensitive company information

### Current state of employee security awareness

Awareness of the insider risk, however, is not influencing many companies represented in this study to put practices in place that will improve the security culture and training of employees. Only 35 percent of respondents say senior executives believe it is a priority that employees are knowledgeable about how data security risks affect their organizations. As a result, 60 percent of respondents believe employees are not knowledgeable or have no knowledge of the company's security risks.

### Employee training programs falling short

While every company surveyed has a training program, many of these programs do not have the depth and breadth of content to drive significant behavioral changes and reduce the insider risk. Only half of the companies agree or strongly agree that current employee training actually reduces noncompliant behaviors.

Forty-three percent of respondents say that training consists of only one basic course for all employees. These basic courses often do not provide training on the risks that lead to data breaches. The following are critical areas that are often ignored:

- Less than half (49 percent of respondents) say the course includes phishing and social engineering attacks

- Only 38 percent of respondents say the course includes mobile device security

- Only 29 percent of respondents say the course includes the secure use of cloud services

Further, only 45 percent of respondents say their organizations make training mandatory for all employees. Even when mandatory, exceptions are made for certain individuals. Specifically, 29 percent of respondents say the CEO and C-level executives in their companies are not required to take the course. Not only does this set a poor example for other employees, it puts high value and sensitive information at risk due to the potential carelessness of senior executives.

**Missing a valuable learning opportunity**

Following a data breach, companies have a unique opportunity to affirm through training the importance of being conscientious when handling sensitive and confidential information as well as having a real example of the consequences of a data breach. Unfortunately, 60 percent of companies do not require employees to retake security training courses following a data breach, missing a key opportunity to emphasize security best practices.

**Conclusion: Creating a culture of security**

Mitigating the insider risk should include both culture and training. Sixty-seven percent of respondents say their organizations do not provide incentives to employees for being proactive in protecting sensitive information or reporting potential issues. Only 19 percent of respondents say their organizations provide a financial reward and 29 percent of respondents say they include such information in performance reviews.

Another approach to changing behavior is to have clear consequences for negligent behavior. Unfortunately, the survey found that one-third of respondents say there are no consequences if an employee is found to be negligent or responsible for causing a data breach. The most common type of follow-up with the employee is a one-on-one meeting with a superior. Only 16 percent of respondents say the employee's salary would be reduced and 33 percent say the employee would be terminated.

In conjunction with culture, DPPT programs are critical to reducing the insider risk. Programs should have content that addresses the security risks facing the organization. Following are two recommendations that will improve both training and culture.

**Training.** Gamify training to make learning about potential security and privacy threats fun. Interactive games that illustrate threats for employees can make the educational experience enjoyable and the content easier to retain. For example, new technologies that simulate real phishing emails and provide simple ways to report potentially fraudulent messages are gaining traction. These types of real-time and interactive activities can be effective in changing user behavior.

**Culture.** Apply the carrot and stick approach to reducing the insider risk. Provide employees with incentives to report security issues and safeguard confidential and sensitive information. Companies should establish and communicate the consequences of a data breach or security incident caused by negligent or careless behavior. The tone at the top is critical to strengthening an organization's security culture. Senior executives should set an example by participating in the DPPT program and emphasizing the importance of reducing the risk of a data breach or security incident.

## Part 2. Key findings

In this section, we provide an analysis of the key findings. The complete audited findings are presented in the appendix of the report.

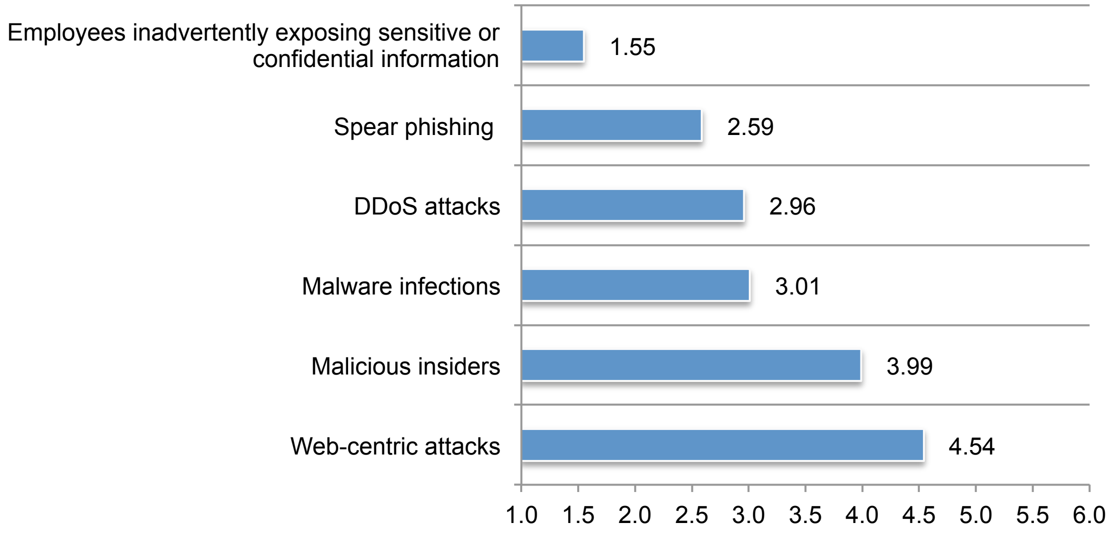
We have organized the report according to these topics:

- Insider risk & data breaches
- Organizational culture & insider risk
- Training programs & technologies to reduce insider risk

### Insider risk & data breaches

**The number one security risk is employee carelessness**. We asked respondents to rank their concern regarding six security risks. As shown in Figure 2, the number one concern is employees inadvertently exposing sensitive or confidential information followed by spear phishing and DDoS attacks.

**Figure 2. Which security risks are you most concerned about?**
1 = most concern to 6 = least concern



# Amid Yahoo hacks, a churn of security officers

By Wendy Lee

December 22, 2016 Updated: December 22, 2016 9:15pm

2

Photo: Win McNamee, Getty Images

IMAGE 1 OF 3
Alex Stamos, Yahoo information security chief (left); Google manager George Salem and Craig Spiezle, Online Trust Alliance founder, at a Senate committee.

When Yahoo experienced the nation's largest hacking attack, with information stolen from more than 1 billion user accounts in August 2013, it lacked a permanent information security chief.

The Sunnyvale company has struggled to retain top cybersecurity executives. Since 2012, Yahoo has had three chief information security officers — a role responsible for guarding against hacking threats and patching weaknesses quickly. For roughly a year, the company was searching for someone to permanently fill the position. That's when the record-breaking breach occurred.

Yahoo's churn of security executives may seem rapid, but it is only slightly faster than what's considered normal among large companies. The average tenure of chief information security officers is 2.1 years, according to the Ponemon Institute, a research firm. Often those who serve in these roles are heavily recruited by other firms, because executives with the right skill set are scarce. But as massive data breaches become more frequent, concern has mounted that the lack of continuity could cause problems.

“If you have a person leaving every year in essence, I don’t know how you have a continuum that is safe for people,” said Pam Dixon, executive director of the World Privacy Forum, referring to the turnover of information security chiefs at Yahoo. “The company gets hurt and consumers get hurt,” she said.

MORE BY WENDY LEE

**LeEco’s U.S. expansion plans, and finances, under scrutiny**

**Silicon Valley courts cord cutters**

**Verizon could seek discount in buying Yahoo, analysts say**

**Over 1 billion Yahoo accounts had data stolen in 2013 breach**

Since 2012, the year CEO Marissa Mayer joined the company, Yahoo has invested more than $250 million in security initiatives, according to the company. In the past two years it has paid $2 million in cash to security researchers as part of a program to catch bugs in its software.

“Today’s security landscape is complex and ever-evolving, but, at Yahoo, we have a deep understanding of the threats facing our users and continuously strive to stay ahead of these threats to keep our users and our platforms secure,” Yahoo said in a statement. The company declined to make

Bob Lord, Yahoo's chief information security officer since November 2015, available for an interview.

During Mayer's tenure, Yahoo experienced two enormous data breaches — the one in August 2013 that affected more than 1 billion user accounts and a separate incident in 2014 impacting at least 500 million accounts. The company said it still does not know what caused the August 2013 breach and believes a state-sponsored actor was behind the 2014 hack. Security experts say it's possible the hacks could have happened to any company, but Yahoo could have taken additional steps to protect users. For example, some of the data taken from users in 2013 were scrambling passwords using MD5, which is considered an outdated technology because software tools can uncover the actual passwords, experts said. (The company switched to a more secure way of scrambling passwords in summer 2013.)

"(It's) very easy to crack," Apostolos Giannakidis, a lead security engineer at Waratek, which specializes in application security, said of MD5. "Yahoo should have made the effort to upgrade their infrastructure."

Mayer was hired to turn the company around, with a focus on building and revamping the company's sites and apps to increase its users and generate more advertising dollars. Yahoo spent more than

$2.3 billion on acquiring promising tech firms to bring new technology and talented people in to the business. But her efforts had mixed results, and a push by activist shareholders resulted in Yahoo planning to sell its Internet properties to Verizon, a $4.8 billion deal that could be in jeopardy because of the two massive data breaches — which Yahoo did not disclose or apparently even know about when it negotiated the original deal with Verizon.

As Yahoo focused on building products, security seems to have lagged. Yahoo's chief information officer in 2014 and 2015, Alex Stamos, suggested end-to-end encryption for messages, meaning that only the people corresponding with each other, not Yahoo, could read what was written. But Jeff Bonforte, who oversees Mail, opposed that because "it would have hurt Yahoo's ability to index and search message data," according to the New York Times.

"I'm not particularly thrilled with building an apartment building which has the biggest bars on every window," Bonforte told the Times.

Yahoo says its Mail and security teams are collaborating on end-to-end encryption.

Stamos, who is now Facebook's chief security officer, declined through a Facebook spokesman to be interviewed.

At many tech firms, the security team is often separate from the engineers building products, analysts said. Sometimes security workers will make suggestions that may slow down an app but increase protections.

“There is just a natural tension between those two, and undoubtedly Yahoo, like a lot of groups, got caught in the middle,” said James Lee, chief marketing officer at Waratek. “The people that are developing those apps have security on their checklist, but they are focused on getting the app in on time, on budget with the right features and functionality.”

Jeremiah Grossman, chief of security strategy at SentinelOne who worked at Yahoo from 1999 to 2001, said there were times in that much earlier era when the security team only learned of new products when the press release came out, and it was a rush to try to fix vulnerabilities after they launched.

“It’s like trying to change a tire when you’re going 50 miles (an hour),” Grossman said. “It’s much easier when the car is stopped.”

Several factors play into why top cybersecurity executives move around so much, but one of the most common issues is lack of funding for their priorities, according to a Ponemon Institute survey of large companies' chief information security officers.

"When you are in the middle of a financial crisis or challenge, naturally you want to spend money on things (that) raise the top line or reduce the bottom line," said Michael Fey, Symantec's chief operating officer and president. "Cybersecurity is neither."

The median compensation package for chief information security officers was $308,880 in fiscal year 2015, according to executive compensation research firm Equilar.

"For these type of people, it is less about compensation and benefits and it's more about the challenge," said career counselor Nick Parham. "It's very frustrating for these men and women to see the problem or see a possible fix and not gain C-level approval to fund it and fix it."

More companies started hiring senior-level security officers seven or eight years ago, as data breaches became more common, according to the Ponemon Institute. But the position is still relatively new, with just 40 percent of large companies having a fully dedicated chief information security officer, the institute said in a 2014 presentation. That statistic has since improved, but most companies still do not have a dedicated chief information security officer, according to Larry Ponemon, the institute's founder.

By contrast, “you’re not going to find a company that doesn’t have a CFO (chief financial officer),” Ponemon said during the 2014 presentation.

In the future, some analysts believe that more information technology professionals will need to be trained on cybersecurity to increase the pool of experts. Smaller firms may want to hire contractors of services specialized in security.

Parsing candidates can be hard, since there isn’t a specific training or certification program that cybersecurity executives need to go through. And while security chiefs generally take the fall for data breaches, the mere fact of a breach does not necessarily mean that the security chief — who may be constrained by budgets or other factors — did a poor job.

“Just understanding who is great at their job and who’s not is sometimes difficult,” Fey said.

*Wendy Lee is a San Francisco Chronicle staff writer.*
*Email: wlee@sfchronicle.com Twitter: @thewendylee*

# Understaffed and at Risk:
## Today's IT Security Department

**Sponsored by HP Enterprise Security**

Independently conducted by Ponemon Institute LLC

Publication Date: February 2014

# Understaffed and at Risk: Today's IT Security Department

January 2014

## Part 1. Introduction

One of the biggest barriers to a strong security posture, according to Ponemon Institute research, is having a team of security professionals that can deal with complex and serious internal and external threats to the organization. *Understaffed and at Risk: Today's IT Security Department* was conducted by Ponemon Institute and sponsored by HP Enterprise Security to understand how effective organizations are in hiring and keeping enough skilled and expert staff to meet their IT security mission.

The study focuses on how organizations are attracting and retaining qualified IT security professionals. Topics included:

- How the demand for skilled IT security personnel has changed since 2012.
- The number of jobs that go unfilled because of difficulties in finding qualified personnel.
- The length of time spent on the job and the problem of high turnover, especially among the more senior security practitioners.
- Compensation packages that might not be adequate to attract and keep staff.
- The most desirable skills and backgrounds for security staff.

We surveyed 504 human resources and IT security specialists in the United States. To ensure a knowledgeable respondent, we only permitted individuals to complete the survey who are responsible for attracting, hiring, promoting and retaining IT security personnel within their organizations.

Some key findings from this research include:

- The IT security function is understaffed. Seventy-percent of respondents say their organizations do not have enough IT security staff.

- The average headcount of an IT security function is expected to grow from 22 staff members in 2013 to 29 in 2014.

- On average, 58 percent of senior staff positions in IT security went unfilled in 2013. Respondents are somewhat optimistic that the hiring of senior IT security personnel will improve and the percentage of unfilled positions is expected to decrease to 49 percent in 2014.

- On average, 36 percent of staff positions went unfilled in 2013. In contrast to filling senior-level positions, the percentage of unfilled staff positions is expected to increase to 40 percent in 2014.

- Senior security executives don't stay in their jobs very long. On average, CISOs and others in a similar position leave after 2.5 years. Those in a technician or comparable role stay an average of 4 years.

- Decisions about IT security staffing and recruitment are most likely made by human resources and corporate IT.

- On-the-job experience and professional certifications make the biggest difference when hiring a security practitioner. Most job recruiting takes place at conferences.

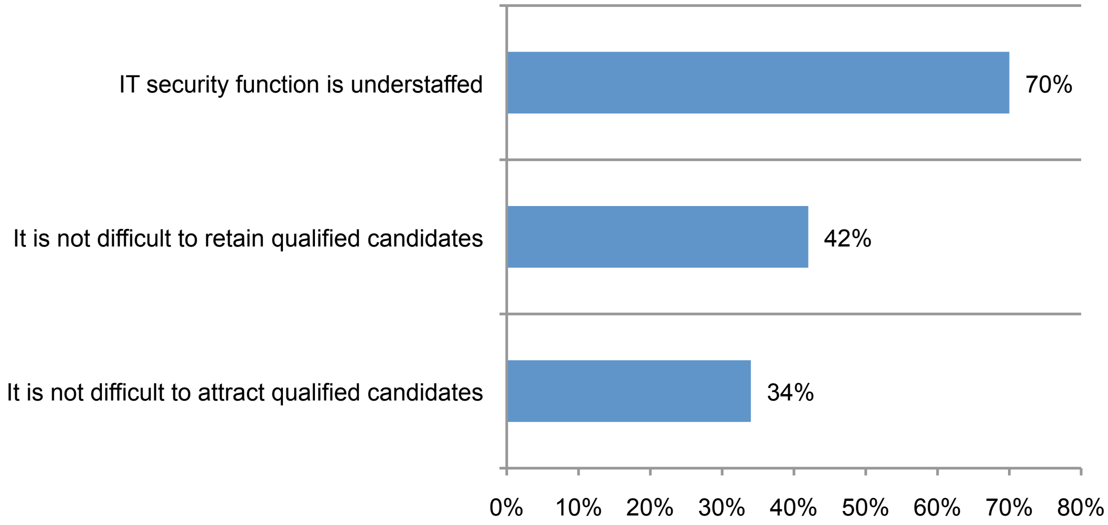
- By far, salary is the most important part of a hiring package. Key to stopping turnover is the ability to offer a competitive salary.

## Part 2. Key Findings

Following is a summary of the key findings. The complete audited findings are presented in the appendix of this report.

**Most organizations in this study do not have the depth and breadth of qualified security professionals.** According to Figure 1**,** the majority of respondents (70 percent) say their organization's IT security function is understaffed. Only 34 percent say they have no difficulty in attracting qualified candidates and 42 percent say they have no difficulty in retaining these experts.

**Figure 1. Challenges to staffing the IT security function**
Strongly agree and agree response combined



# Mitigating the Cybersecurity Skills Shortage

## Top Insights and Actions from Cisco Security Advisory Services

# Cybersecurity Skills Are in High Demand, Yet in Short Supply

Increasingly sophisticated threat campaigns. High-profile data breaches. Determined threat actors. The sophistication of the technology and tactics used by criminals has outpaced the ability of IT and security professionals to address these threats.[1] *Security Magazine* reports that "most organizations do not have the people or systems to monitor their networks consistently and to determine how they are being infiltrated."[2] Cisco estimates there are more than 1 million unfilled security jobs worldwide.[3]

Determined attackers and persistent threats are only part of the cybersecurity skills problem. According to new research from Cisco, there is a disconnect between the perception and reality of security preparedness. While many chief information security officers (CISOs) believe their security processes are optimized–and their security tools are effective–their security readiness likely needs improvement.[4] This disconnect, along with rapidly evolving regulatory requirements and networking technology, will further widen the cybersecurity skills gap.

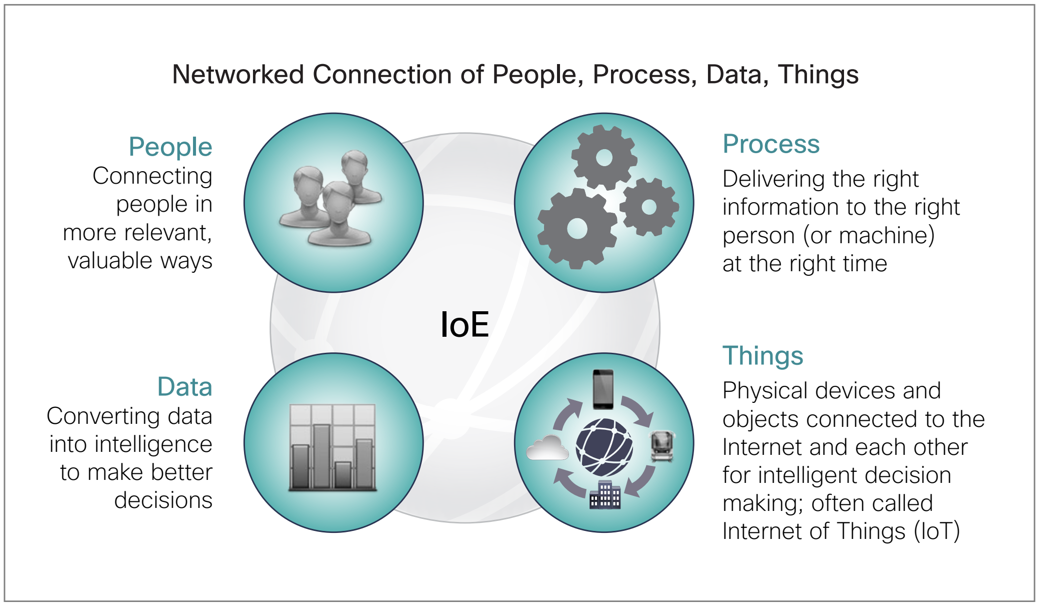
Cybersecurity hiring challenges will also be impacted by the Internet of Everything (IoE), which represents an unprecedented opportunity to connect people, processes, data, and things (Figure 1). While IoE will create new operating models that drive both efficiency and value, it may also become the world's most challenging cybersecurity threat.[5] Why? As customers embrace IoE, they must bring together IT and operational technology, giving adversaries new targets such as vehicles, buildings, and manufacturing plants.

> *Threats to critical OT (operational technology) infrastructure are no longer theoretical and their existing vulnerability is an area that actors are actively exploiting.*[6]
>
> – Michael Assante

This blurring of IT and operational technology environments has already resulted in a 250 percent spike in industrial automation and control system incidents over the past 4 years.[7] According to Gartner, the number, scale, and sophistication of operational technology attacks will continue to increase, putting connected industrial systems, building control systems, and energy systems at risk.[8] "Mitigating advanced persistent threats in OT environments requires people who can bridge IT and OT," says Jon Stanford, principal, Cisco® Security Solutions. People who can bridge the gap between IT and OT are in extremely short supply.

Against this dynamic backdrop, Cisco Security Services offer important insights and recommended actions that can help you mitigate the cybersecurity talent shortage.

Figure 1. With the IoT, Organizations Must Secure a Greater Attack Surface



Networked Connection of People, Process, Data, Things

People
Connecting people in more relevant, valuable ways

Process
Delivering the right information to the right person (or machine) at the right time

Data
Converting data into intelligence to make better decisions

Things
Physical devices and objects connected to the Internet and each other for intelligent decision making; often called Internet of Things (IoT)

> *"There is going to be a Black Friday–like buying frenzy for cybersecurity talent throughout 2015 ... Some organizations will be left high and dry."*[9]
>
> – Jon Oltsik

> *As the Internet of Things (IoT) gains more traction, the lack of basic security standards in IoT devices will exacerbate the security skills gap.*[10]

## Insight Number 1

## Cybersecurity Requires Cyber Strategies

Too many companies today have underperforming security programs because of a failure to define and execute holistic cybersecurity strategies. "A good cyber strategy should be a living, breathing, constantly questing process–not a task that is done every 6 months," says Brian Tillett, principal, Cisco Security Solutions. The lack of a cohesive, enterprisewide cybersecurity strategy, one that is based on policy, typically results in improvised security solutions that leave in-house security teams playing Whac-A-Mole. According to the *Cisco Security Capabilities Benchmark Study*, internal security teams spend 63 percent of their time on security-related tasks, leaving them little time to drive strategic security initiatives (Figure 2).[11]

## Insight Number 2

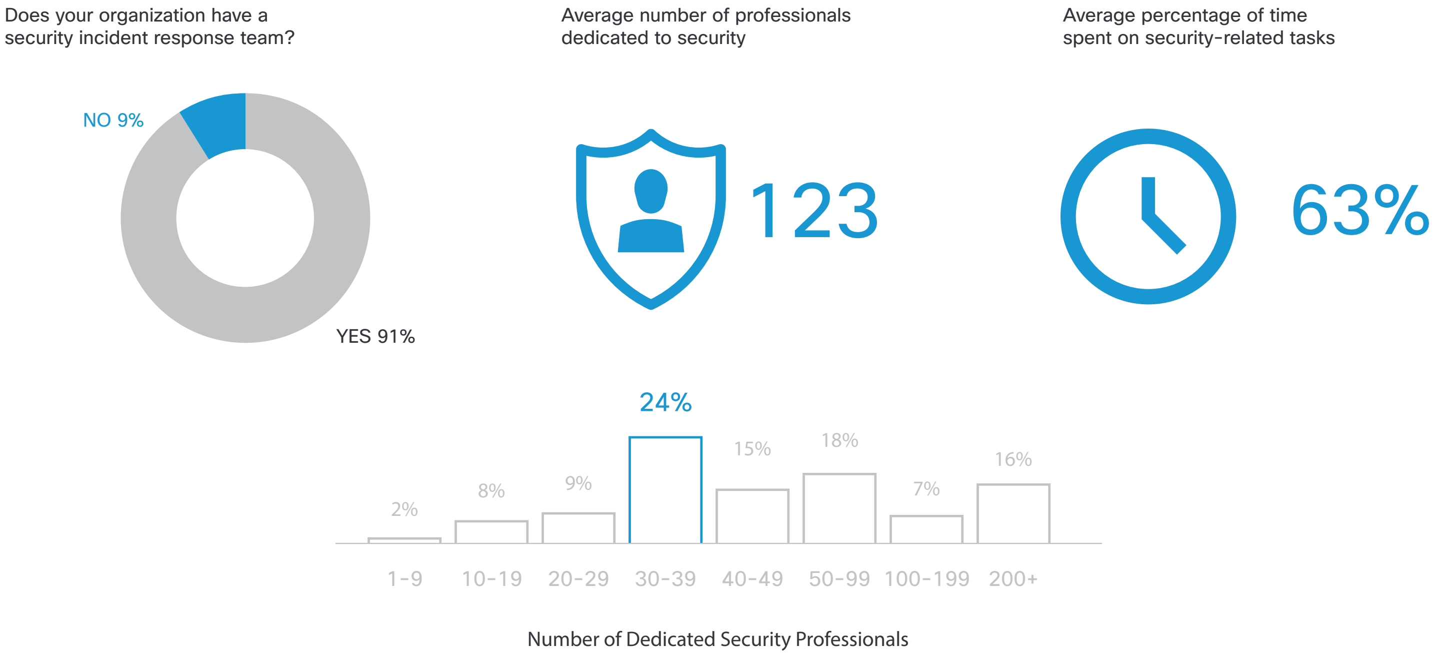
## Security Organizations Need Data Scientists with Business Acumen

With so many high-profile, high-cost breaches, business leaders are beginning to take notice. *Network World* says, "We're starting to see more executive-level emphasis on cybersecurity, more resources coming into cybersecurity, across all industry sectors. That has definitely increased the demand for cybersecurity folks."[13]

> *"Executive management and boards of directors are now recognizing that cybersecurity is not just a tech problem. It's a business problem."*
>
> – Ann Bednarz quoting Charlie Benway

As security discussions move to the boardroom, CISOs and their teams need data science skills to analyze cybersecurity data and business skills to manage trust (company reputation) and risk (costs). The new CISO must communicate not in bits and bytes, but in plain language. "The conversation has migrated from one of red, yellow, and green vulnerability status checks to financial conversations in which security risk is measured in dollars and cents," says Dmitry Kuchynski, principal, Cisco Security Solutions. "CISOs must be able to frame the discussion in a strategic way that clearly communicates the potential impact of a data breach on stock price, customer loyalty, customer acquisition, and the brand."

Figure 2. Security Resource Snapshot[12]



Does your organization have a security incident response team?

Average number of professionals dedicated to security

Average percentage of time spent on security-related tasks

### Insight Number 3

## The Cyber-Talent Skills Gap Will Drive Enterprises to Managed Security Services

Most organizations are struggling to solidify a cybersecurity vision supported by an effective strategy that uses new technologies, simplifies their architecture and operations, and strengthens their security team.[14] This is pushing companies to bolster in-house cybersecurity expertise with professional security services (Figure 3).

> *More than 50 percent of organizations today seek advice or consulting services to help with their security strategies.*[15]

Using security partners and managed security service providers (MSSPs) who continually invest in security expertise, intelligence, and innovative new technologies is a great way to keep pace with a dynamic threat environment. According to Jon Stanford of Cisco, "A trusted security advisor can help you establish a cybersecurity policy foundation and develop an effective cybersecurity program with the appropriate governance based on those policies." They can also take the burden of detection and triage off your hands, so your in-house security team can focus on remediation.

### Insight Number 4

## Effective Cybersecurity Requires People, Analytics, Intelligence, and Technology

Solving the growing cybersecurity problem requires more than skilled security professionals. It requires a combination of people, advanced analytics for proactive threat hunting, comprehensive intelligence for real-time threat awareness, and integrated security architectures.

This is why, according to Jon Oltsik of Network World, enterprises are shifting toward a new security model, one that is characterized by "central command-and-control and distributed enforcement, anchored by security intelligence and analytics." Oltsik writes that this relatively new technology model is "more art than science," and "CISOs need help in all areas of their planning here: design, test, implementation, integration, support, etc."

> *"Large organizations don't want to buy more one-off threat management point tools from a potpourri of vendors."*
>
> – Jon Oltsik

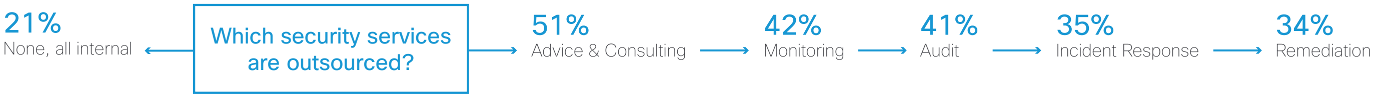
### Insight Number 5

## Every Company Is a Security Company

Security concerns are now top-of-mind not only for companies, but also for consumers. Cisco calls it "the trust problem." Simply put, breaches undermine confidence in both public and private organizations. This trust erosion leads to a decline in customer confidence in the integrity of your products. Without trust, customers will go elsewhere. As a result, all businesses need to think about security as their mainstream business.

Maintaining trust through state-of-the-art security capabilities can help you stand out in a crowded market. Innovative security-enabled solutions–such as mobile payments, virtual and automated advice, and customer collaboration tools–can create more valuable and relevant interactions. Differentiated security helps reassure customers and increase loyalty, and it can help you win in the IoE economy.

Figure 3. Findings from *Cisco Security Capabilities Benchmark Study*



# Recommended Actions for Security Professionals

**Action Number 1**

## Get a Cybersecurity Strategy

Dmitry Kuchynski of Cisco recommends that you "treat cybersecurity as if it were one of your solutions or services. When it comes to investor and customer confidence, security is just as important to the business." Cybersecurity strategies should be holistic. They should be:

- **Developed in collaboration with critical business units** – If your strategy is created in a vacuum, it will not align with business needs. Brian Tillett of Cisco recommends that you "embed security personnel into business units, so security strategy can be baked in instead of bolted on."
- **Focused on business growth** – If you bring value with your strategy, security becomes a business differentiator and revenue generator, transforming security from a cost center to a growth center.
- **Validated at the board level** – Executive leadership that prioritizes security is one of the signs of security sophistication, according to the *Cisco Security Capabilities Benchmark Study*. Keeping company executives informed and involved in data breach preparedness and response plans is essential for maintaining a sophisticated security posture.
- **Dynamically managed** – Threat actors continuously adapt. Your cybersecurity strategy should, too. Treat it like it is a living, breathing, constantly questing process. If you let it languish, your threat posture also suffers.

In addition, Jon Stanford recommends thinking broadly when formulating your strategy: "Cybersecurity is not just about IT. Your strategy has to include OT." Stanford also recommends performing risk assessments on third-party vendors, because you are only as good as your weakest link.

**Action Number 2**

## Get a Breach Plan and Advanced Cybersecurity Skills

Even firms with mature security organizations and advanced security protocols will experience breaches, according to the Ponemon Institute. Every organization needs an incident response plan—a plan that maps out in advance and regularly tests against the types of incidents most likely for the firm's threat model.[16]

The Ponemon Institute recommends that you clearly define accountability and responsibility for data breach response and that it not be dispersed throughout the company. Instead, Ponemon advises creating cross-functional teams that include the expertise necessary to rapidly respond to a data breach. An effective incident response plan requires the skills of a variety of functions such as IT security, legal, and public relations.

Managed services from a trusted security advisor can help you create an incident response plan: one that uses the latest skills, analytics, intelligence, and technology to ensure rapid and effective resolution. Just make sure your security advisor or MSSP has deep knowledge of global enterprises.

You should take advantage of cybersecurity courses from vendors and certification groups to bolster in-house skills. The Cisco Learning Network now offers a new Cisco Cybersecurity Specialist certification for people who want to take on a first-responder role when networks have been attacked. Global Information Assurance Certification (GIAC) has a new Network Forensic Analyst certification that gives security professionals the skills to extract and analyze artifacts and activity left behind from unauthorized activity or network-based attacks.

**Action Number 3**

## Get Security on the Agenda in the Boardroom

When it comes to getting executives engaged, Brian Tillett says, "Don't ever let a good breach go to waste." Tillett recommends using high-profile breaches as an opportunity to have a conversation with the board. Describe how that breach can happen in your organization. Then show them how to address vulnerabilities.

When it comes to finding CISOs with the business acumen to effectively engage with high-level executives, Dmitry Kuchynski recommends looking beyond security professionals for in-house hires: "Top-level candidates today come from military or federal enforcement background, corporate technology, and security strategy experience because they have an understanding of the threat environment and bring a strategic mindset to the table." Kuchynski also recommends considering corporate security professionals who are moving laterally from small to large organizations and IT professionals who have made the move from the infrastructure to the security domain. If you are not successful in your CISO talent search, Kuchynski recommends partnering with a trusted vendor.

### Action Number 4

## Keep Your Security Solutions Operating at Peak Performance

Less than 50 percent of respondents in the *Cisco Security Capabilities Benchmark Study* use standard automation tools for identity administration or user provisioning, patching and configuration, penetration testing, endpoint forensics, and vulnerability. Greater use of automation tools not only improves your security posture, it frees your security staff to focus on more strategic initiatives.

Brian Tillett recommends the following: "Turn on more of the security features already integrated into your solutions. Organizations typically turn on only 30 percent of the security features available to them. This is a tremendous underutilization of security resources that can make already-constrained security teams more productive and existing security solutions more effective."

And keep your software current. Unpatched or outdated software represents an attractive attack surface for adversaries. According to Cisco security research, "The proliferation of outdated versions of exploitable software will continue to lead to security issues of great magnitude."[17]

### Action Number 5

## Choose the Right Partners

If every company is now a security company, choosing the right partner is paramount. Obtaining the right cybersecurity partner can help you round out your expertise, so you can be:

- **More dynamic in your approach to security** by benefitting from global best practices and real-time threat intelligence
- **More proactive in your security posture** by using advanced analytics capabilities
- **More adaptive and innovative than your adversaries** by implementing a threat-centric security program that can address the full attack continuum before, during, and after an attack across all attack vectors

> *"In advanced security analytics, the value comes from the people. Software does not provide the answers; it provides the tools and delivers the data needed to discover answers."*
>
> – *"Big Data" Analytics in Network Security*, Frost & Sullivan, Feb. 13, 2015[18]

## For More Information

These are just a few of the many ways organizations can mitigate the cybersecurity skills shortage:

- Find more information about Cisco Security Services.
- Read the *Cisco 2015 Annual Security Report*.
- Get an overview of Cisco Advisory Services.
- Learn how the Cisco Managed Threat Defense Service can help you navigate a changing threat landscape.
- Find out more about the new Cisco Cybersecurity Specialist certification.

[1] *Cisco 2015 Annual Security Report*, Cisco, Jan. 20, 2015.

[2] "Why the Security Talent Gap is the Next Big Crisis," *Security Magazine*, May 2014.

[3] *Cisco Security Capabilities Benchmark Study*, Cisco, Oct. 2014.

[4] *Cisco 2015 Annual Security Report*, Cisco, Jan. 20, 2015.

[5] *Cisco 2014 Annual Security Report*, Cisco, Jan. 20, 2015.

[6] "Cyber Threats Providing Their Power over Power Plan Operational Technology," PowerMag.com, Feb. 1, 2015.

[7] "Cyber Threats Providing Their Power over Power Plan Operational Technology," PowerMag.com, Feb. 1, 2015.

[8] "Operational Technology Security and the Challenges Ahead for 2015," Gartner Blog Network, Dec. 29, 2014.

[9] "Cybersecurity Skills Shortage Panic in 2015?," *Network World*, Dec. 9, 2014.

[10] "2015 Security Predictions: IoT to Join Cloud Breaches and Ransomware," ZDNet, Dec. 19, 2014.

[11] *Cisco Security Capabilities Benchmark Study*, Cisco, Oct. 2014.

[12] *Cisco Security Capabilities Benchmark Study*, Cisco, Oct. 2014.

[13] "Shortage of Security Pros Worsens," *Network World*, March 9, 2015.

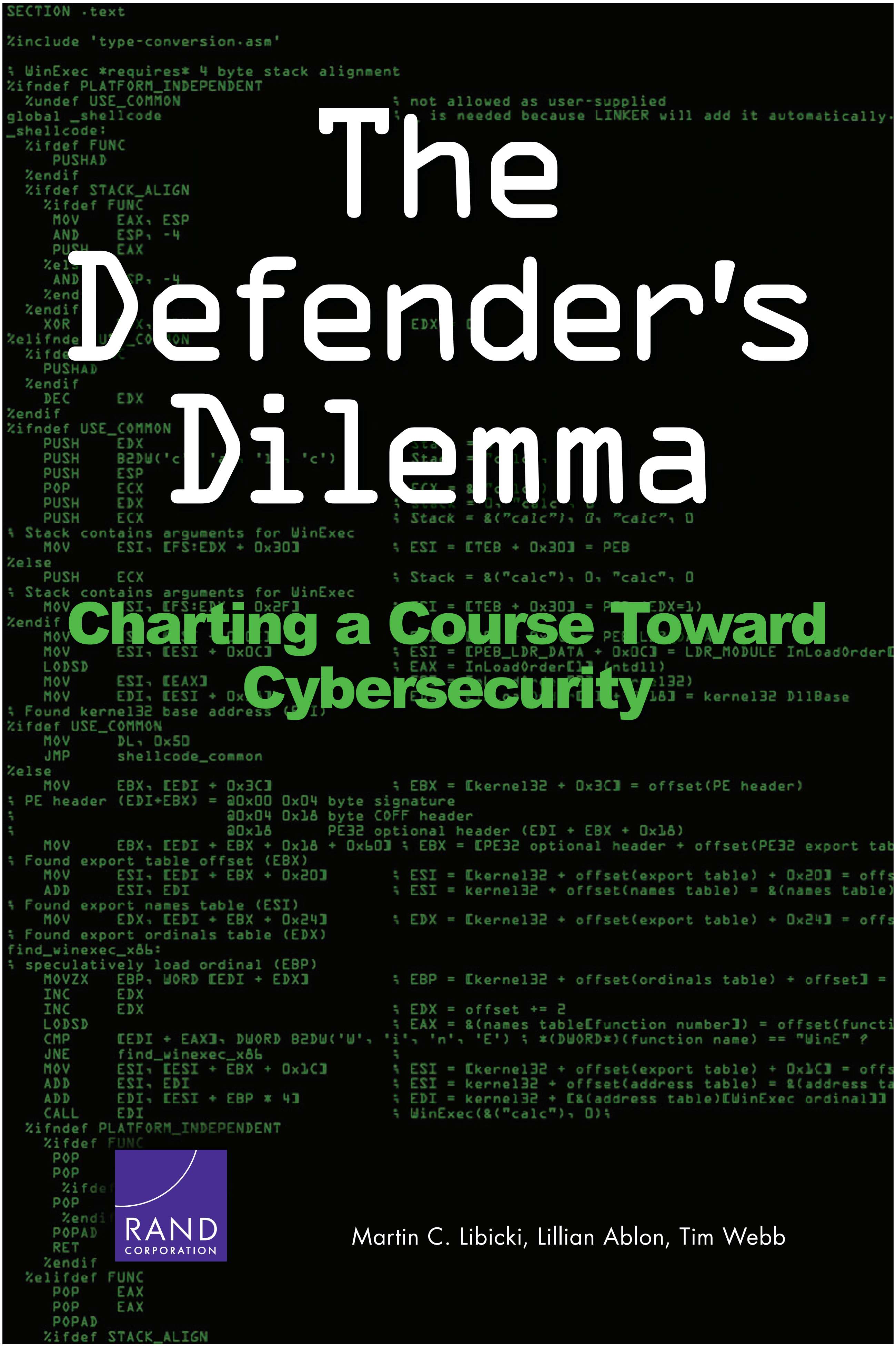
[14] *Cisco 2014 Annual Security Report*, Cisco, Jan. 16, 2014.

[15] *Cisco 2015 Annual Security Report*, Cisco, Jan. 20, 2015.

[16] *Ponemon Institute Report: Cyber Security Incident Response – Are we as prepared as we think?*, Ponemon Institute, Jan. 2014.

[17] *Cisco 2015 Annual Security Report*, Cisco, Jan. 20, 2015.

[18] *"Big Data" Analytics in Network Security: Computational Automation of Security Professionals*, Frost & Sullivan, Feb. 13, 2015.



# The Defender's Dilemma

## Charting a Course Toward Cybersecurity

RAND CORPORATION

Martin C. Libicki, Lillian Ablon, Tim Webb

For more information on this publication, visit www.rand.org/t/rr1024

Library of Congress Cataloging-in-Publication Data
ISBN: 9780833089113

Published by the RAND Corporation, Santa Monica, Calif.

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

# Summary

Cybersecurity is, in part, a world of secrecy. Organizations charged with protecting information from disclosure are understandably prone to concealing at least some of the practices used to hide that information. Further, the world of cybersecurity suffers from short-sighted analysis: There is great debate about what malefactors are doing to networks, but less discussion about the short- or long-term effects of this activity. Malicious hackers, whose success requires subverting computers, are certainly not putting out statistics on their activity. Moreover, surprise is endemic to cyberattack.[1] Compromising an assiduously defended system or network (or subverting diligently written software) is often accomplished by finding a path in that has eluded the attention of those charged with keeping such paths closed. Since defenders rarely let known holes go unpatched for very long,[2] the success of a hacker often depends on finding an unknown (or at least unwatched) hole—tantamount to a surprise.

Thus, there is a great and urgent need to understand the evolution of the cybersecurity space. The Gartner research firm estimates that worldwide spending on cybersecurity is approaching $70 billion per year (Giles, 2014) and is growing at roughly 10 to 15 percent annu-

[1] The use of the term *cyberattack* in this report encompasses the traditional definition of the word, as well as the current media use of the word—i.e., affecting an entity's network to attack in the traditional sense (disrupt, deny, degrade, destroy, or deceive); conduct intelligence, surveillance, and/or reconnaissance; and exploit or exfiltrate data or information.

[2] This statement takes into account systems that work around the clock and thus cannot be taken down easily for maintenance.

ally with no deceleration in sight. Despite this, it would be an understatement to say that organizations are dissatisfied with existing cybersecurity—and there is scant confidence among defenders that their exertions will give them the upper hand against malicious hackers two to five years out. Many believe that hackers are gaining on defenders. This combination of rising expenditures and questionable success creates a sense that security efforts cannot continue on this course.

Our purpose in this report is to understand the fundamental forces driving cybersecurity. To this end, we have interviewed chief information security officers (CISOs), reviewed the cybersecurity industry's slate of cutting-edge products, and assessed the struggles of the software industry (and its foes) to make or (alternatively) break secure software. With this background, we used heuristic modeling to illustrate how some of these forces might interact with one another. We conclude with some lessons for organizations and public policymakers on how to promote cybersecurity in a cost-effective manner.

In doing so, we bring several assumptions into play.

*First*, the proper goal of a cybersecurity program (or policy) is to minimize the combined cost of expenditures on cybersecurity plus the expected costs arising from cyberattacks (e.g., network or facility down-time, costs of recovery, loss of reputation). This is difficult to measure, however. Organizations can measure what they spend on cybersecurity but can only guess at the costs their security measures have saved, for a couple of reasons. Not only is it difficult to prove a negative (an attack prevented), but many of these costs can be tricky to calculate—notably the often-mentioned impact of a potential cyberattack on an organization's reputation.[3]

*Second*, malicious hackers are also sensitive to costs and benefits, and they understand how to respond to market signals (Ablon, Libicki, and Golay, 2014). They weigh the relationship between the effort associated with penetrating and exploiting a system and the gains from doing so—gains that, incidentally, are generally much lower than the costs to the organization that has been hacked. The harder a system is to infiltrate,

[3] There are those, however, who aim to summarize the costs. Ponemon Institute (2013a), for example, puts out a report each year on the average cost of a data breach.

the more effort hackers must put into cracking it; for some systems, such efforts may be deemed unprofitable. Similarly, if systems were harder to crack, fewer hackers would be capable of breaking into them, and those who could might have other priorities. But for an organization defending itself against a state intelligence apparatus determined to access it, a system has to get fairly close to being impenetrable to be secure.

*Third*, although cyberattacks vary greatly, many of them, particularly those associated with advanced persistent threats, tend to have two important stages. One is achieved when attackers penetrate client systems (e.g., computers of end users). The other is achieved when attackers leverage the penetration of client systems to move throughout the victim network and compromise their target. Keeping hackers from penetrating client systems depends on a multitude of factors, but attention can be given to the quality of software on the client systems themselves (e.g., web browser add-ons). Keeping penetrated client systems from compromising the network may be a matter of adroitly administered software and/or services that implement a security watch over the entire system.

*Fourth*, because malicious hackers are thinking adversaries, many measures to improve security beget countermeasures. The extent to which these countermeasures negate all, some, or none of the initial measures' improvements can vary greatly. We concentrate on two measure-countermeasure contests. The first focuses on investments made in tools to discern the activities of hackers within organizations contrasted with the techniques that hackers use to operate below the visibility of such tools. The other contest deals with efforts to reduce the exploitable faults in the software stack and how those measure up to the tools and techniques used by hackers to find and exploit such faults (although some hackers do wear white hats in this case, enough wear black hats to ensure this contest is no game).

## Findings

As a result of interviewing 18 CISOs, we drew three sets of conclusions: those we expected, those that confirmed our suppositions, and those that came as surprises.

The conclusions we expected were as follows:

- Security postures are highly specific to company type, size, etc., and there often are not good solutions for smaller businesses.
- The importance of intellectual property varies with the individual firms' missions.
- Cybersecurity is a hard sell, especially to chief executives.
- Although CISOs generally lack a way to know whether they are spending enough on cybersecurity, they split between those who think spending is sufficient and those who feel more is needed.
- Air-gapping, wherein networks are electronically isolated from the Internet, can be a useful option. (In a softer form, it is compatible with tunneling through the Internet but otherwise not interacting with it).
- Responding to the desire of employees to bring their own devices (BYOD) and connect them to the network creates growing dilemmas.
- CISOs feel that attackers have the upper hand, and will continue to have it.

The conclusions that confirmed our suspicions were these:

- Customers look to extant tools for solutions even though they do not necessarily know what they need and are certain no magic wand exists.
- When given more money for cybersecurity, a majority of CISOs choose human-centric solutions.
- CISOs want information on the motives and methods of specific attackers, but there is no consensus on how such information could be used.
- Current cyberinsurance offerings are often seen as more hassle than benefit, useful in only specific scenarios, and providing little return.
- The concept of *active defense* has multiple meanings, no standard definition, and evokes little enthusiasm.
- CISOs lack a clear vision on incentives.

- Information-sharing tends to live within a web of trust.
- CISOs tend to be optimistic about the cloud, but, apart from those who sell cloud services, most are willing to be only cautious fast followers.
- CISOs are likely to assign lower priority to security-as-a-service offerings.
- CISOs, in general, are not ready to concentrate their purchases from a single vendor (but also are not sure that heterogeneity is the best solution, either).

The conclusions that came as surprises were the following:

- A cyberattack's effect on reputation (rather than more-direct costs) is the biggest cause of concern for CISOs. The actual intellectual property or data that might be affected matters less than the fact that *any* intellectual property or data are at risk.
- In general, loss estimation processes are not particularly comprehensive.
- The ability to understand and articulate an organization's risk arising from network penetrations in a standard and consistent matter does not exist and will not exist for a long time.

The contest between measures (new security capabilities) and countermeasures (attempts to undermine those capabilities) is escalating and has been evolving for quite some time. To take just one example, basic firewall filtering yielded to finer-grain signature-based examination with intrusion detection and prevention systems and deep packet inspection. As companies learned that they needed to reduce not only the likelihood but also the impact of attacks, they turned to data loss prevention (DLP) programs and more-expansive use of virtual private networks (VPNs). Attackers, in turn, made more use of stealth, obfuscation, and malware polymorphism. Defenders shifted to detecting attacks based on network behaviors and not signatures. Sometimes the same tools and techniques were used by both defenders and attackers. As the novelty and innovation of each new technique was met with new countermeasures, it became harder to distinguish those that worked well from those that were merely added complexity and noise, thereby taxing an organization's limited time and resources. Without metrics, it is unclear why consumers would pay more for good products over merely adequate ones. And the best tools and largest resources could not get around the many security weaknesses that arose from human nature.

If network and software architectures were static, defenders would eventually gain the upper hand—but innovation is the lifeblood of the information technology sector. Similarly, if networks were inherently more complicated, systematic progress might be made toward security. "Walled garden" software systems (where the provider controls all aspects of content and transactions) have generally proven harder to attack than open systems. But the trend over the past 20 years has been in the other direction—greater reliance on open systems for both software and networking.

The bedrock of cybersecurity is good system software. Companies often find themselves having to invest in defensive measures because foundational systems and software are unsecure. The security and solidness of the actual software helps to prevent attackers from gaining a foothold on a network (what we call the *external hardness* of an organization). But once they are in, additional defenses are then required to prevent attackers from converting that foothold into something that hurts the organization (what we call the *internal hardness* of an organization). As it is, software vulnerabilities and weaknesses arise through design (architectural) or implementation (coding) faults. A subset of these vulnerabilities is *exploitable*, in that an attacker can perform some sort of unintended action with the ultimate goal being remote code execution (giving an actor full control over a target's system). Sometimes, these software vulnerabilities are found and fixed before release. Other times, the vendor discovers the vulnerabilities after customers have the product and provides patches. Still other times, researchers not tied to the vendor can discover these (zero-day) vulnerabilities;[4] when they do, their options include informing the vendor (white markets), selling the information to

[4] A *zero-day vulnerability* is one for which no patch has been developed (usually because the vendor of the software is unaware that the software has that particular vulnerability).

governments or their suppliers (gray markets), or selling the information to cybercriminals (black markets). Because finding the vulnerabilities is nontrivial, doing so can fetch a great deal of money. Unfortunately, fixing such vulnerabilities often introduces new problems—and even when it does not, malware and attacks spike after disclosure of these vulnerabilities and even after the release of a corresponding patch.

However, software design trends indicate that there might one day be enough improvement to raise questions about the assumption that attackers have to be defeated within the network (minimizing damage) rather than before they get into the network (preventing damage). The three most frequently used Internet browsers (Internet Explorer, Firefox, and Chrome) are evolving to where corrupted web pages create faults that propagate only within the browser rather than the operating system. Further, operating systems and browsers themselves are improving (in large part because patching has become more automated) and require increasingly sophisticated campaigns to infect.

Conversely, there are burgeoning sets of network relationships arising from the Internet of Things (IoT) and from the many privileges that organizations conclude they must extend to other organizations.[5] These make the perimeter harder to identify, thus harder to guard, and means that cybersecurity efforts must be based on the assumption that bad guys are already in the network and that security has to be managed even more intensively at the systemic level, rather than focusing on keeping attackers out of a system in the first place.

We used the results of our analysis to construct a heuristic model for cybersecurity as a way of framing the problem and allowing some systematic treatment of its underlying factors. We drew our basic variables from all three aspects of our research, paying particular attention to the concerns and the methods used by CISOs and the measure-countermeasure struggles.

[5] *Internet of Things* refers to a near future when every electronic or even electrical device (e.g., a microwave oven) is connected to the Internet.

Our model portrays the struggle of organizations to minimize the cost arising from insecurity in cyberspace (over a ten-year period). Those costs are defined as the sum of

- losses from cyberattack
- direct costs of training users
- direct cost of buying and using tools
- indirect costs associated with restrictions on the ingestion of BYOD/smart devices
- indirect costs of air-gapping particularly sensitive subnetworks.

Calculations were carried out for year 0 (assume it to be 2015) and iterated for each year over a subsequent ten-year period. Changes over time include the number and vulnerability of computers and devices, shifts in the losses associated with cyberattacks, the introduction of new tools, and the declining efficacy of some tools in the face of countermeasures. The odds that an organization was successfully attacked in a given year were deemed to be a product of an organization's external hardness (its ability to keep attackers from establishing a beachhead within an organization's network) and internal hardness (its ability to keep a beachhead from being converted into a systemic compromise). Its projected losses from cyberattack were the product of those odds of successful attack multiplied by value at risk. In other words, hardness, both external and internal, can be considered as a probabilistic measure. When both external and internal hardness equal 0, an attack is absolutely likely to penetrate an organization, and a penetration is absolutely likely to lead to compromise and hence loss of value at risk. If *either* external hardness *or* internal hardness is 1, either an attack will be stopped at the border or no form of penetration will result in a compromised system.

The model runs five subroutines in a specific order to determine an organization's possible losses from cyberattack. These subroutines represent parameters discussed by CISOs. They are run in sequence, rather than in parallel, to represent a progression from hope to painful commitment:

- We hope that training users suffices.

- If that does not work well enough, we buy cybersecurity tools to thwart attackers.
- If the combination of training and tools does not prove sufficient, we work on restrictions: first, to head off the burgeoning increases in addressable devices; second, to ensure that at least the most critical processes are protected through isolation.

Each affects one of the three parameters: external hardness, internal hardness, and value at risk.

- First, the odds that every computer and smart device (something as intelligent as, but not used as, a computer in the traditional sense) can repel an attacker are calculated based on the number of computers and devices and the quality of their software. This determines an organization's initial external hardness.
- Second, an organization can improve its external hardness by increasing the level of training (think also of restrictions on users' ability to make changes to their own machines and/or access organizational assets).
- Third, an organization's internal hardness is enhanced to the extent that it buys cybersecurity tools.[6]
- Fourth, an organization can increase external hardness by successively reducing the number of connected devices it supports, in large part by restricting what employees can bring into the network (as a practical matter, other policy tools are also available, including those that determine which devices are visible to the outside).
- Fifth, an organization can reduce the cost of a cyberattack by isolating parts of its networks where compromise might be particularly costly.

The model yields a plethora of results, of which the following merit note:

[6] In practice, companies have to use these tools intelligently, and many do not. An attribute applied to organizations, diligence, captures the difference between those who use cybersecurity tools well and those who do not.

- The various instruments that organizations can use to control the losses from cyberattack are collectively powerful. Yet much of what they do is to transfer costs from losses to defenses: Roughly one-third of the reduced losses are offset by increased costs associated with using such instruments (direct acquisition and usage costs plus implicit reduction in the value of networking). Developing instruments that offer better cost-effectiveness ratios would be important.
- The size of the organization matters greatly to its optimal strategy. Small organizations benefit from circumstances and policies that reduce their attack surface (e.g., BYOD/smart device policies). Larger organizations need a panoply of instruments to keep costs under control. One size does not fit all.
- The quality of software used by organizations is an important exogenous factor in determining their susceptibility to penetration. There need to be better mechanisms to convey the interests that organizations have in the quality of code to those responsible for getting the code into products.
- Over time, the potential influence of devices on cybersecurity will approach and perhaps exceed the influence of computers on cybersecurity. The introduction of networked computers into organization in the 1980s and 1990s was allowed to happen without a very sophisticated understanding of the security implications. The same mistake ought not be made with intelligent devices.
- Tools that do not lend themselves to countermeasures (e.g., better configuration management) are likely to retain their usefulness in the long run. By year 10, of the top dozen tools (out of 30), only one was a tool of the sort that could be subject to countermeasures (and that was a tool introduced in the last year of the model). If measures are taken to increase the number of tools available to organizations—which, as the model suggests, can cut losses substantially—then the choice of such tools should take the slower obsolescence of such tools in mind (vis-à-vis, for instance, those that seek to differentiate the signal of attack from the noise of background).

## Organizational and Policy Lessons

Our research leads us to draw one set of lessons for organizations and a separate set for policymakers.

### Organizational Lessons

- **Know what needs protecting, and how badly protection is needed.** Part of self-knowledge is understanding what is worth protecting; in that regard, it was striking how frequently a corporation's reputation was widely cited by CISOs as a prime cause for cybersecurity spending. Another part is knowing what machines are on the network, what applications they are running, what privileges have been established, and with what state of security. The advent of the IoT (smart phones, tablets, and so forth) compounds the problem.
- **Know where to devote effort to protect the organization.** A core choice for companies is how much defense to commit to the perimeter and how much to internal workings. Attackers often establish a persistent presence in networks when an employee opens a bad attachment or goes to a malicious website. Once penetrated, weaknesses in other code enable the malicious code either to execute its own instructions or obey those of the attacker. Better code would make this process much more difficult. But infections are possible even with better code, so multiple tools must be employed.
- **Consider the potential for adversaries to employ countermeasures.** Mounting a defense is a necessary first step. But as defenses are installed, organizations must realize they are dealing with a thinking adversary and that measures installed to thwart hackers tend to induce countermeasures as hackers probe for ways around or through new defenses. This tit-for-tat exchange will eventually drive measures toward increasing expense, additional complexity, and, arguably, less reliability. Corporations should think about installing measures of the sort that are less likely to attract countermeasures.

### Policy Lessons

By and large, CISOs we interviewed did not express much interest in government efforts to improve cybersecurity, other than a willingness to cooperate after an attack. Yet it seems likely that government should be able to play a useful role. The question is what sort of role would be mutually beneficial and perceived as such. One option is to build a body of knowledge on how systems fail (a necessary prerequisite to preventing failure) and then share that information. The government plays a similar role in the aviation and medical fields. A community that is prepared to share what went wrong and what could be done better next time could collectively educate the world's CISOs and produce higher levels of cybersecurity.

## Conclusions

One conclusion is a seeming paradox: The amount of pessimism expressed over cybersecurity is cause for hope. One result of this dour view is that CISOs are both more numerous and more influential than they were five years ago, let alone ten. Core software is improving, and cybersecurity products are burgeoning. The combination is likely to make the attacker's task more difficult and more expensive—which will not solve the problem, but will make it more manageable.

Hurdles remain, of course. Our earlier work, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar,* pointed out that hackers who knew how to infiltrate networks but not how to take criminal advantage of that infiltration are now trading expertise with those who do. This union makes the business of hacking more profitable—and, thus, more attractive. Second, the IoT might provide hackers with many more pathways to exploit. Still, while the challenges are formidable, they are not insurmountable, and those who defend networks are engaged fully.

# Acknowledgments

RAND reports typically draw on a wide collection of supporters, collaborators, and helpers in their creation. We would first like to mention the invaluable insights provided by the numerous experts at Juniper Networks and Edelman Corporation. Within RAND, Cynthia Cook and Henry Willis have been wise and patient in their assistance and insight to this project. Our reviewers, Herb Lin and Bradley Wilson, offered sage advice that improved the report.

Finally, we are exceptionally grateful to the 18 chief information security officers and the numerous bug bounty directors, zero-day market vendors, and other computer security professionals who took the time to share their insights and provide their input on the cybersecurity landscape.