radware

SECURITY AND THE C-SUITE

THREATS AND OPPORTUNITIES

Findings & Analysis from
Radware's Executive Application
& Network Security Survey

TABLE OF CONTENTS

01 Executive Summary

Radware, in partnership with Merrill Research, surveyed CIOs and senior vice presidents of IT, network or security in the United States and the United Kingdom. The goal: to understand their greatest challenges, threats and opportunities when it comes to information security. This Executive Application & Network Security Survey complements Radware's 2015-2016 Global Application & Network Security Report with insights and perspectives from the C-suite. In this report, Radware presents its key findings and analysis—along with recommendations for mitigating ransomware, security issues related to the Internet of Things (IoT) and other growing threats.

Among the highlights of the Executive Survey:

C-suite awareness is growing.

Given the prevalence of cyber-attacks, it is no surprise that 82% of respondents say that security is now a CEO or board-level concern. In Radware's 2014 research findings, that was true for just under three-quarters of respondents. Meanwhile, 95% of 2016 respondents indicated that security is a very or extremely important priority within their organizations—with 41% reporting that their organization recently implemented a monthly board review of security measures.

Spending is up. So is uncertainty.

Approximately two-thirds of executives reported 10% to 59% increases in cyber-security spending since last year. Yet in both the U.S. and the U.K., more than half of executives did not know exactly how much money and time their company has spent on security. Three-quarters have implemented, or are implementing, an automated security model, and 72% have invested in cyber insurance. Yet they're still losing sleep over a host of uncertainties, including the risk of insider hacks, the growing sophistication of cyber thieves and vulnerabilities associated with home-based workers (42% told us they've recently implemented stricter security policies related to telecommuting).

Pay up—or else.

Radware's *2015-2016 Global Application & Network Security Report* noted significant growth in ransom as motivation for attackers—which increased from 16% in 2014 to 25% in 2015. Even though C-suite executives are unlikely to have full visibility to every security threat, one in seven respondents in the 2016 Executive Application & Network Security Survey reported that they experienced a ransom attack in the past year. More than half (54%) admitted to paying a ransom. In the U.S., the average ransom paid was $7,520; in the U.K., it was significantly higher at £22,218.

"Nothing beats a poacher turned gamekeeper."

In the face of increasingly complex threats, a growing number of companies are open to employing ex-hackers. In fact, 23% of respondents have already invited hackers to test their company systems—and another 36% said they would be willing to do so.

IoT security is top of mind.

Executives in both the U.S. and the U.K. cited network infrastructure and IoT devices as the two most likely targets for hackers. Radware identifies two major risks: that IoT devices will fuel new network vulnerabilities and that devices could be "taken over" by bots in order to steal sensitive information, launch attacks or enable other nefarious activities.

Suppliers and partners could be a weak link.

Among respondents, 44% have been including suppliers and partners in security processes for more than two years. Another 33% have begun doing so within the past two years. However, more than one-fifth (22%) are still not addressing suppliers and partners in their processes at all. When Radware asked what partners and customers are asking related to enhanced security, about two-fifths of executives said "none" or gave no specific answer.

02

Security Risk is Business Risk

As noted in Radware's *2015-2016 Global Application & Network Security Report*, more than 90% of Security Industry Survey respondents reported experiencing attacks in 2015. In the 2016 Executive Application & Network Security Survey, respondents underscored the growing cost of cleaning up after a security attack. More than a third of respondents in the U.S. said an attack had cost them more than $1 million, and 5% said they spent more than $10 million. Costs in the U.K. were generally lower, with 63% saying an attack had cost less than £351,245 (or about $500,000), though 6% claimed costs above £7 million.

Estimated Cost of an Attack

	COUNTRY	
	U.S.	**U.K.**
Less than $100,000/Less than £70,249	15%	12%
$100,001-$250,000/£70,250-£175,622	14%	34%
$250,001-$500,000/£175,623-£351,245	18%	17%
$500,001 but less than $1M/£351,246-£702, 490	16%	10%
$1M but less than $3M/£702,500-£2.1 million	14%	12%
$3M but less than $5M/£2.1 million but less than £3.5 million	9%	9%
$5M but less than $10M/£3.5 million but less than £7 million	8%	1%
$10M+/£7 million or more	5%	6%

Figure 1: Estimated Cost of an Attack

Given the prevalence and cost of security incidents, it is not surprising that four out of five executives (82%) say that security threats are now a CEO or board-level concern. That's a notable increase from the 2014 survey, which found that security was a CEO or board-level concern for less than three-quarters of respondents.

The Executive Survey affirmed that partners remain an area of potential weakness. Every partner that interacts with a business or its network should adhere to the same security standards. To their credit, 44% of respondents have been including suppliers and partners in security processes for more than two years. Another 33% have begun doing so within the past two years. However, more than one-fifth (22%) are still not addressing suppliers and partners in their processes. When asked what partners and customers are asking related to enhanced security, about two-fifths of executives said "none" or gave no specific answer.

Radware's Executive Survey also confirmed the potential impact of security threats. Executives rated brand reputation, operational loss and revenue loss as the areas of greatest impact. Among the other potential effects cited: productivity loss, impact on share price value, unexpected increases in budget, training/education and hiring requirements, and contract loss. The impacts selected were largely the same among U.S. and U.K. executives, with one exception. Business leaders in the U.K. were more likely to mention unexpected contract loss as a top concern.

Security Threats are a Board Level Concern

The majority of respondents indicate that security threats are now a CEO or board-level concern in their company.*

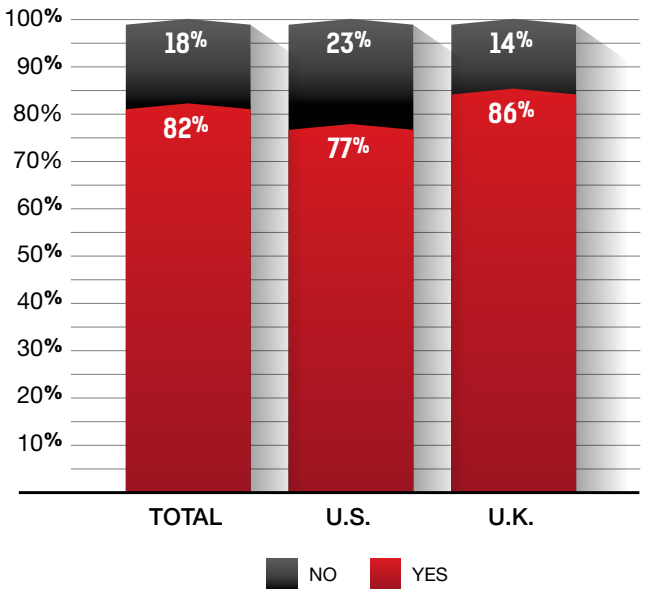

Figure 2: Security Threats Are a Board-Level Concern

* This is slightly higher for those in the U.K., compared to those in the U.S.

Impact of Security Threats on Business

		COUNTRY	
RANKED 1st/2nd	TOTAL	U.S.	U.K.
Brand Reputation Loss	34%	38%	31%
Operational Loss	31%	31%	32%
Revenue Loss	30%	34%	27%
Productivity Loss	24%	27%	21%
Share Price Value	18%	16%	20%
Unexpected Budget Increases	17%	14%	19%
Unexpected Training/Education	16%	16%	16%
Unexpected Hiring Requirements	15%	14%	16%
Unexpected Contract Loss	15%	10%	20%

- Security threats are most likely to cause the biggest losses to a company's brand reputation, operations, and revenue.
  - These areas are rated as first or second in terms of greatest impact by executives.
- Executives in the U.S. and U.K. rate the impacts similarly with the exception of unexpected contract loss which is more likely to be rated as a greatest or second greatest impact compared to those saying the same in the U.S.

Figure 3: Impact of Security Threats on Business

Above all, the Executive Survey confirmed that companies continue to take action—but still have opportunities to do more. In both the U.S. and the U.K., about one-third of executives rate changes in technology, C-level awareness or knowledge/education as critical to effectively thwarting security threats. Process and policy changes are extremely important to almost three in 10 executives, with just one in five pointing to changes in resources as critical to dealing with security threats.

Importance of Changes to Thwart Security Threats

EXTREMELY IMPORTANT (CRITICAL)	TOTAL	COUNTRY	
		U.S.	U.K.
Changes in Technology	35%	36%	34%
Changes in C-Level Awareness	33%	34%	32%
Changes in Knowledge/ Education	32%	31%	34%
Changes in Process	28%	31%	26%
Changes in Policy/ Procedure	28%	32%	24%
Changes in Resources	22%	19%	24%

- About one-third of the executives rate changes in technology, C-level awareness, or knowledge/education as extremely important/critical in effectively thwarting security threats.
- Process and policy changes are extremely important to almost three in ten executives, and about one in five say changes in resources are critical in dealing with security threats.
- Importance is consistent between the U.S. and the U.K.

Figure 4: Importance of Changes to Thwart Security Threats

03

To Pay or Not to Pay: Ransom-Based Threats on the Rise

Businesses face growing threats from ransom-based attacks. These attacks have two primary "flavors":

- **Ransomware** – in which attackers typically use malware to encrypt critical data, making it unusable until the user complies with instructions to make a payment via Bitcoin. One of the latest varieties to emerge is Ransom32, which is ransomware as-a-service that gives cyber criminals a jumpstart on holding victims' information hostage.

- **DDoS for ransom** – in which attackers send their target a letter that threatens a DDoS attack at a certain day and time unless the organization makes a payment (usually $2,000 to $10,000) via Bitcoin. Often hackers will launch a small-scale attack as a preview of what could follow.

Previous Radware research revealed an increase in ransom-oriented attacks, which accounted for about one-quarter of motivations in 2015 (versus 16% in the prior year). In the full-length *2015-2016 Global Application & Network Security Report*, Radware predicted that ransomware and DDoS for ransom schemes would continue to affect everything from traditional enterprises to cloud companies. The findings of the most recent Executive Survey underscore the validity of that prediction.

Among those who have not experienced a ransom situation, the majority—77% in the U.S. and 91% in the U.K.—say they would not pay. Yet among those who actually experienced a ransom attack, response varies among U.S. versus U.K. executives. Interestingly, 64% of U.K. executives reported paying a ransom, more than double the 29% in the U.S. who said the same. For those who paid, the average ransom in the U.S. was $7,560 versus £22,218 among the organizations that paid attackers in the U.K. (Note: Those averages do not include those with ongoing situations.)

Paying Ransoms

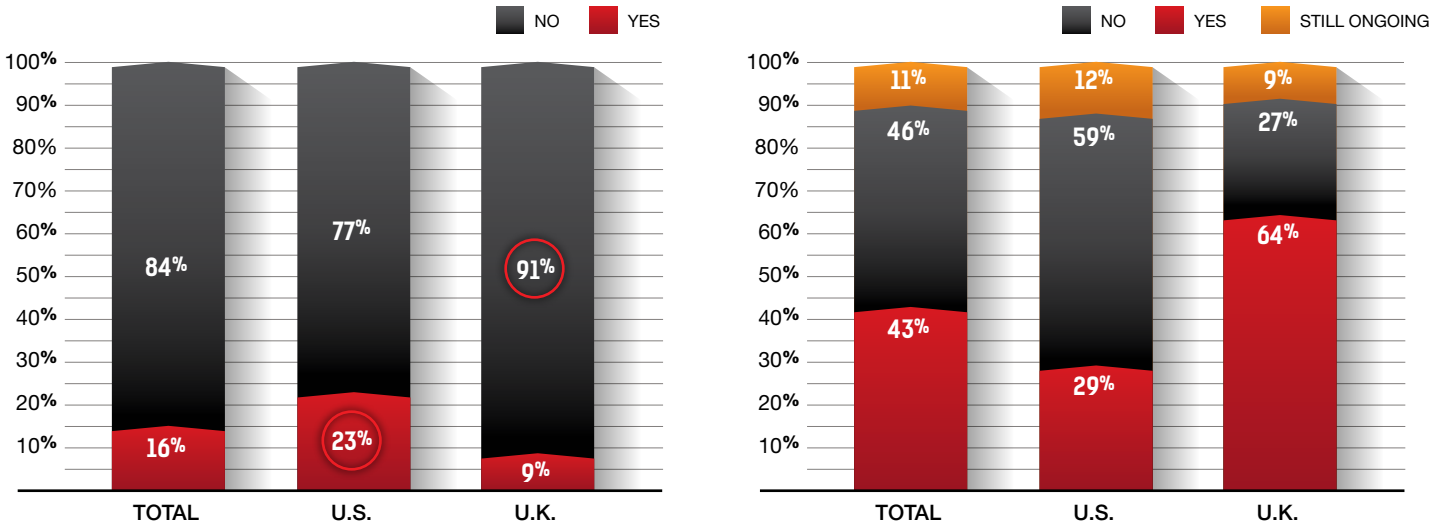

Figure 5: Paying Ransoms

- Among those who have not experienced a ransom situation, the majority say they would not pay a ransom.
- Among the few who have experienced a ransom attack, more than half in the U.S. did not pay, while almost two-thirds in the U.K. did pay. One respondent indicated that paying did not guarantee that the attacker would do their part.
- The average ransom across the five in the U.S. who indicated they paid the ransom was $7,560 compared to £22,218 among the seven who paid in the U.K. (This does not include those with ongoing situations.)

Across industries and geographies, the propensity to send funds could reflect a strong desire to make the threat "go away" by simply giving in to the demands. That action may have the unintended—and undesirable—consequence of inviting continued ransom threats. If word gets out on the "dark web" that a company paid, it can expect to receive additional threats from the same or different attackers. After all, negotiating with criminals can become a proverbial slippery slope.

Radware saw that firsthand through its client ProtonMail—the Swiss-based encrypted email provider. In November 2015, the company experienced consecutive attacks initiated with a ransom request by hacker group The Armada Collective. Hoping to stop the attacks, ProtonMail paid a ransom, only to see the attacks continue with volumetric and burst attacks combining application and network vectors.

The Kansas Heart Hospital in Wichita learned a similar lesson in May 2016. Having fallen prey to ransomware, the hospital paid the ransom to get its files back. Instead, it received only "partial access," along with a demand for more funds. The hospital declined the second request. Its experiences were the latest in a string of ransomware attacks targeting hospitals and health systems across the U.S.

In addition to The Armada Collective, other groups have emerged at the forefront of this trend, including DD4BC and ezBTC Squad. One of the newest players is Kadyrovtsy (named after the elite forces of the Kadyrov administration in Chechnya), which recently threatened two Polish banks and a Canadian media company. Meanwhile, “copycats” are compounding the headaches. These players are issuing fake letters—hoping to translate empty threats into fast profits.

What now?

While it is impossible to predict the next target of a ransom group, organizations need to proactively prepare their networks and have an emergency plan in place for such an incident. If faced with a threat from a blackmail group, it is important to take the proper steps to mitigate the attack. Organizations under attack should consider:

- A security solution that can protect an infrastructure from multi-vector attacks, including protection from network and application-based DDoS attacks, as well as volumetric attacks that can saturate the Internet pipe.
- A cyber-security emergency response plan that includes an emergency response team and process. Identify areas where help is needed from a third party.
- Monitoring security alerts and examining triggers carefully. Tuning existing polices and protections to prevent false positives and allow identification of real threats when they occur.

How can you detect a fake ransom letter?

- **Assess the Request**
  The Armada Collective normally requests 20 Bitcoin (approx. $6,000 US Dollars at the peak of the attacks), while other campaigns have been asking for amounts above and below this amount. Fake hackers request different amounts of money. Low Bitcoin ransom letters are most likely from fake groups who are hoping their price point is low enough for someone to pay rather than seek help from professionals.
- **Check Your Network**
  Real hackers prove their competence by running a small attack while delivering a ransom note. If you can see a change in your network activity, the letter and the threat are probably genuine.
- **Look for Structure**
  Real hackers are well organized. Fake hackers, on the other hand, don’t link to a website. Nor do they have official social media accounts.
- **Consider Other Targets**
  Real hackers tend to attack many companies in a single sector. Fake hackers are less organized, targeting anyone and everyone in hopes of making a quick profit. Contact peers or information sharing organizations in your industry to see if there is a more widespread campaign underway.

04

IoT: Internet of Things or Internet of Threats?

In Radware's Executive Survey, respondents clearly identified the Internet of Things as one of their top security concerns. Thirty-three percent of executives in the U.S and 29% in the U.K. cited it as an "extremely likely" target in the next three to five years.

Top Security Threats

EXTREMELY IMPORTANT (CRITICAL)	TOTAL	COUNTRY	
		U.S.	U.K.
Network Infrastructure	31%	33%	29%
Internet of Things (IoT) Devices	29%	35%	24%
State Utilities or Nuclear Deterrents	25%	28%	23%
Connected Home	22%	24%	21%
Energy/Power Infrastructure	22%	27%	17%
Connected Cars	20%	22%	18%
Wearables (Fitbits, Garmins, Jawbones, etc.)	18%	21%	14%
Airplanes	17%	23%	10%

Figure 6: Top Security Threats

Two sides to the IoT security coin.

The Internet of Things includes a vast and ever-growing array of networked devices—including smart meters used by utilities, medical devices for monitoring patients' conditions and delivering care, as well as to sensors that do everything from supporting public safety to automating manufacturing processes. When it comes to security and the IoT, Radware sees a two-part dilemma.

The first part: mitigating the risk of vulnerabilities created or compounded by networked devices. Organizations must consider the possibility of a huge increase in unknown vulnerabilities at the device level, as most lack antivirus or advanced endpoint and threat detection capabilities. While sensors and other IoT devices can fuel exponential improvements in speed, accuracy and efficiency of information collection, they also can make a business vulnerable to intrusions and attacks. Even a company's network carrier can be affected if attackers use IoT devices to generate massive spikes in network traffic.

The other side of the IoT security dilemma is being protected from devices—that is, addressing the risk of the "things" themselves becoming vehicles for an attack. For example, in the past utility customers may have worried that a meter reader would forget to close a back gate, leaving the house unsecure. These days, they want assurance that they're not letting a nefarious robot into their homes—putting data privacy and personal safety in jeopardy. On a broader scale, hackers could potentially take control of thousands of smart meters, wreaking havoc on the electrical grid.

Healthcare is another area where vulnerabilities could be devastating. Imagine a patient receiving an email that threatens to alter his or her pacemaker's performance unless a ransom payment is made. It may sound far-fetched, but healthcare has become a frequent target. Already, numerous attacks have blocked hospitals' and other providers' access to their own data. Networked medical devices provide another potential avenue for such schemes.

Mitigating the threat of 'things'.

Regardless of an organization's interests around the IoT, the time has arrived to start taking proactive steps to ensure security. In the end, the full vision of the IoT may or may not come to pass, or it may take longer than some predict. What is undeniable is that connectivity is exploding. While most people may be unaware of how the IoT functions, they will expect it to be secure. Similarly, they will be largely clueless to the potential impact they (and their new gadgets) have on the threat landscape, and thus cannot be relied upon to maintain security capabilities on these devices. As a result—and as underscored by the findings of Radware's Executive Survey—the burden of protecting organizations from the possible wave of new, larger threats falls to the security operations teams.

'Fingerprinting' devices

With the advent of billions of non-traditional IT devices, accurate device identification will simultaneously become more important and more difficult. The primary tool that has long been used for device and user identification—namely, IP addresses—is rapidly declining in its security value.

Dynamic IP addresses, global Network Address Translation (NAT) and anonymous proxies are just a few of the tools out there that are making the connection of IP address and device or user very hazy.

One potential solution is device fingerprinting—a rapidly growing technology that employs various tools and methodologies to gather IP-agnostic information about the source, including running a JavaScript on the client side. The device fingerprint uniquely identifies a web tool entity by combining sometimes dozens of attributes of a user's device to identify and then track activities, generating a behavioral and reputational profile of the user.

05 A Changing Workforce: Automation; Hackers Gain Ground

How will organizations secure themselves against the growing number of increasingly sophisticated threats? Radware's Executive Survey, together with its industry experience, points to potential changes in security talent acquisition strategy and composition.

Automating the front lines.

In the survey, 40% of executives said they've had an automated security model in place for more than two years. Another 35% said they've implemented an automated model within the last two years. Just one-quarter have yet to do so. As published in the *2015-2016 Global Application & Network Security Report*, 38% of respondents reported implementing alert automation following a cyber-attack.

Given the changing nature of security threats—as well as ever-strengthening solution capabilities—the shift toward greater automation is well founded. No one would assert that the design, caretaking or break-fix of information security will ever be fully automated. In fact, it's advisable to invest in quality talent to develop and evolve an organization's security strategy.

Even so, Radware believes that the "front lines" of attack mitigation is going the way of automation. In fact, bots are already taking over a significant portion of network and application security, compliance, cyber-attack mitigation, incident response, disaster recovery, and identity and access management activities. After all, unlike humans, bots don't need to sleep or eat—and they rarely make mistakes. This forces companies to think differently about how they structure their security resources, keeping the human talent at the top of the pyramid and the bot armies on the front lines fighting attacks.

Security Measures

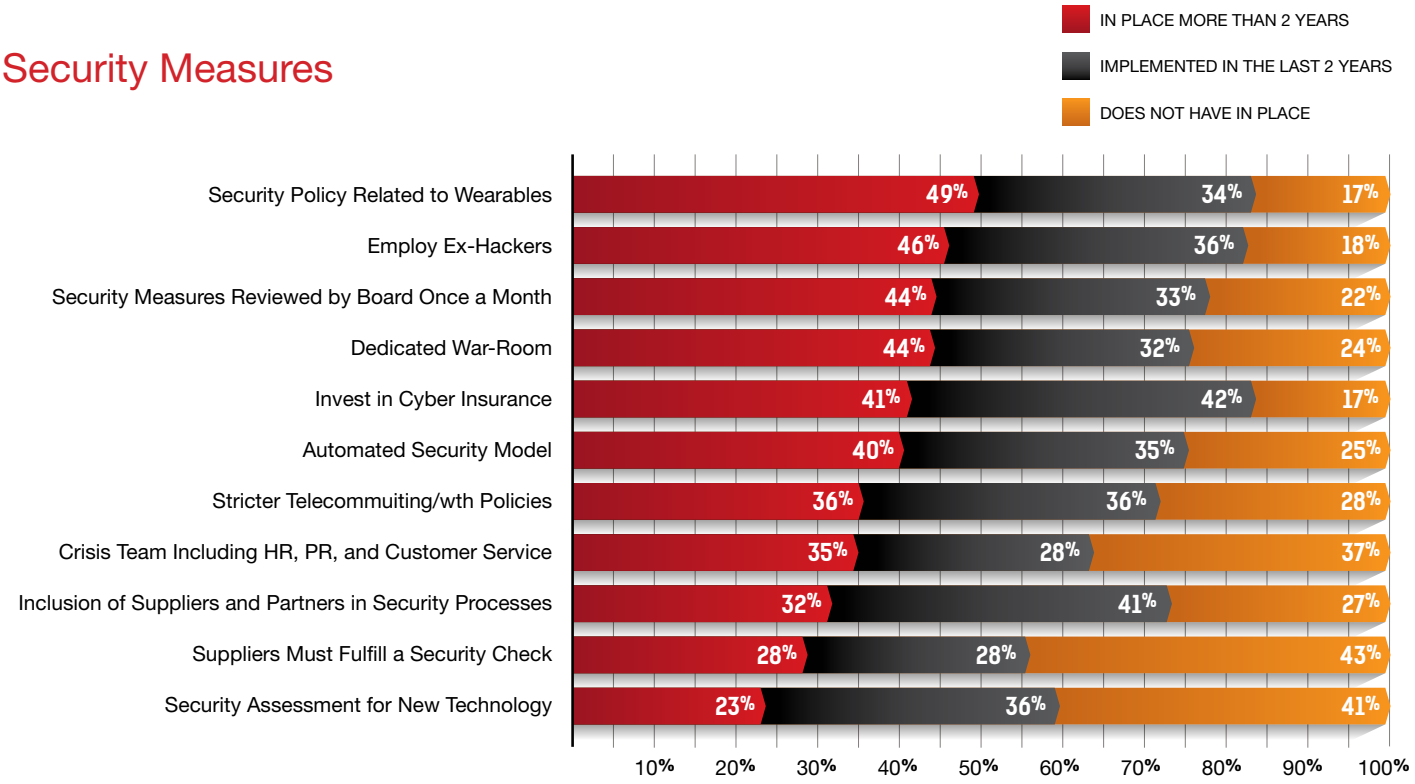

Figure 7: Security Measures

Former criminals: New source of talent?

Historically, there's been some disagreement about the wisdom of using ex-hackers to help test networks and identify vulnerabilities. There's obvious risk in hiring someone who has made a name for himself or herself as a hacker, as these individuals have demonstrated a willingness and ability to break the law. How can a company be certain that a former hacker won't continue criminal behavior once inside the organization?

Executives were quick to acknowledge employee-related internal risks—risks that are only compounded when viewed through the lens of having former hackers on the payroll. Here's what some respondents said when asked what security concerns keep them up at night:

- "Insider attacks because we can't do much to prevent it."
- "Internal staff compromise. We hire more and more Eastern European staff that may be vulnerable."
- "Home-based work. Too easy to hack."

Yet, the findings of the Radware Executive Survey indicate that the practice of hiring former "bad guys" is becoming mainstream. A growing number of organizations are willing to assume the risks in order to capture the potential rewards—including access to the unique mindset and skillset of a hacker. A former hacker can help not only in testing for vulnerabilities but also in responding to attacks. As one respondent put it, "Nothing beats a poacher turned gamekeeper." Indeed, more than a quarter of organizations (28%) have been using ex-hackers for more than two years, and another 28% have begun doing so in the past two years. Why? As another respondent explained, "Because they can think like hackers and know what they would do to prevent [one]."

The growing acceptance of hackers in the workforce is fueling an interesting phenomenon: hacking as a vehicle for professional advancement. While some hackers act solely with malicious intent, others commit the crimes as a means to an end. Seeking to build notoriety, they launch a headline-grabbing attack. They want to be caught—and acknowledged. After serving their time, they transform the crime into a "calling card" for a lucrative and legitimate position in information security. Of course, when interviewing any hacker, employers must weigh the risks and do their best to differentiate the career builders from the career criminals.

06 Leading Through Uncertainty: What Now?

Best practices for security operations will always vary with business and technical dynamics. Even so, some common practices are becoming increasingly important in the face of the evolving threat landscape.

In analyzing the findings of the Executive Survey, Radware identified insights into how well some are doing—and areas where executives may have opportunities to understand and close security gaps.

Practice #1: Perform greater screening on inbound and outbound data.

In the open-ended responses, one executive mentioned future plans to increase screening on the traffic entering and leaving the organization's network. Such screening represents a significant gap for many organizations—and it's becoming increasingly important to address it. Radware has witnessed an increase in SSL/encryption, making inbound attacks more challenging to detect. Meanwhile, outbound traffic, especially when it's encrypted, is often not inspected.

Recommendation: Ensure that network/perimeter protections can inspect encrypted traffic without scale issues. Implement outbound traffic inspection capabilities.

Practice #2: When it comes to security, know what you're spending and why.

Radware's study revealed an interesting paradox. A majority of respondents (82%) indicated that cyber-security is a CEO- or board-level issue. Yet in both the U.S. and the U.K., more than half of executives did not know how much money or time their company has spent on security—from fighting cyber-attacks to implementing safeguards against hackers. Cyber security is simply too important, and poses too much risk, for that lack of executive awareness.

Recommendation: An organization's board and C-suite should assign ownership to ensure transparency on current threats, protection strategy and where/how resources are being used.

Practice #3: When facing a ransom demand, tread carefully.

With ransom attacks on the rise, the survey uncovered another paradox. Eighty-four percent said if they were approached by cyber thieves, they wouldn't pay the ransom. Yet among those who were actually attacked, 54% said they did pay. Giving in to cyber thieves can be risky, as paying ransom may not stop the attack and, in fact, might increase the odds of additional incidents.

Recommendation: Flip the economic equation—investing resources into network, endpoint and application security rather than "donating" money to criminals.

Practice #4: Consider using hackers to test your security.

The Executive Survey shows increased willingness to use hackers, and with good reason. Hackers brings unique experience and insight as companies work to keep pace with changes to threat landscape and with the latest tactics, techniques and procedures.

Recommendation: At a minimum, conduct penetration testing and explore opportunities to engage white hat hackers to make the testing more realistic—and effective.

Practice #5: Automate security.

As the threat landscape becomes increasingly automated, protections need to be, too. Interestingly, in the Executive Survey, 40% say they have had automation in place for two or more years. That finding contradicts input from the Security Industry Survey, in which respondents told us their organization's security is 80% manual. What this suggests is that executives may underestimate the extent to which certain security protections are still manual. That may include manual signature development for new attacks, as well as policy generation and vulnerability scanning/patching on applications.

Recommendation: True automation comes from enabling technology to initiate protections—not feeding data into a Security Information & Event Management (SIEM) system so that a human can make a decision. Explore multi-vector coverage through coordination of security components.

Case in Point: Best Practices in Action

One Radware customer exemplifies information security innovation. It delivers reliable performance for the company's technology backbone, with a DDoS protection strategy that incorporates proactive instead of reactive technology and uses behavioral analysis to minimize impact on legitimate users.

This online retailer's security team also uses a forward-thinking approach for evaluating return on security investments. In most companies, ROI calculations have focused on how much revenue would be lost per hour of downtime, how long it would take to reestablish a site after an attack and the likelihood of an attack taking the site down. More sophisticated analyses might also include cost to the brand—particularly if a company relies on its online presence for revenue.

This Radware customer took a more innovative approach. The security team began to consider how their ability to block bad traffic at the perimeter would positively affect the entire downstream environment. By building strong controls at every level of the infrastructure, the security team can provide tools for the company's infrastructure and operations teams to process only legitimate traffic.

This focus results in a new, often overlooked, formula to measure the financial impacts of DDoS attacks. For DDoS attacks that will not affect the availability of online services, are those malicious attacks worth processing through the entire infrastructure? Aside from downtime, what are the downsides of having this traffic at any time in the infrastructure? Because of the velocity, volume and frequency of DDoS attacks, many data centers are processing massive quantities of malicious data. Processing that "illegitimate" traffic alongside online customers' legitimate traffic has significant operational and financial impact.

Once the security team started to calculate the cost of bad traffic that was now blocked at the perimeter and removed from downstream processing, they could quantify the return—and easily justify—the company's investments in security.

07

About the Research

On behalf of Radware, Merrill Research surveyed 205 IT executives (104 in the U.S. and 101 in the U.K.) in April and May 2016. To participate in the 2016 Executive Application & Network Security Report, respondents were required to be at company with at least $50 million (or equivalent) in revenue and hold a title of senior vice president level or higher. By design, the survey's respondents were equally split between C-level executives and senior vice presidents. About half of the companies in the survey have 1,000 to 9,999 employees, averaging about 3,800.

www.radware.com