TABLE OF CONTENTS

01 Executive Summary
02 The State of Security in the C-Suite
03 Automation Takes a Seat in the Boardroom
04 C-Suite Priorities: Privacy or Profit?
05 Managing Security: In, Out and in Between
EXECUTIVE SUMMARY

Each year, Radware publishes the findings and analysis of our information security industry survey. Designed for the entire security community, the *Global Application & Network Security Report* helps in understanding the threat landscape, potential impact on businesses, levels of preparedness, emerging threats and predictions for the coming year.\(^1\) Complementing that research is Radware’s annual executive survey. In April 2017, we conducted a global survey of C-suite executives. All respondents represent organizations with at least $250 million (or the equivalent) in annual revenue. Our goal: to understand their greatest challenges, threats and opportunities when it comes to cyber security.

This year’s research revealed important global trends, as well as intriguing perceptions and nuances among U.S. and European executives. Among the findings of the 2017 executive survey:

**ATTACK TRENDS ARE GLOBAL—WITH SOME INTERESTING REGIONAL DIFFERENCES**

Consistent with last year’s survey, close to three in five executives indicated that their company had experienced a cyber-attack in the past 12 months. However, when it came to actual volume of attacks, Radware’s security industry survey reported a much higher percentage of front-line security professionals globally (98%) experiencing at least one attack in 2016.

Compared to US executives, European leaders were more likely to report having experienced an attack. Radware believes this finding is not the result of fewer attacks in the US. Rather, it likely reflects cultural differences in how front-line security teams report to their C-suite, more stringent reporting requirements in Europe – or some combination of those factors.

**CYBER SECURITY REMAINS TOP OF MIND, WITH AWARENESS GROWING IN EUROPE**

Overall, 80% of executives affirm that security threats are now a board-level concern. Further, almost all participants (94%) rate security as an extremely or very important priority, with 62% deeming it “extremely important” (a slight increase from last year’s survey, which found just 53% of all executives viewing it as such).

---

\(^1\) View the 2016-2017 Global Application & Network Security Report
While importance in the US remains steady since 2016’s executive survey, European execs rating security “extremely important” increased from 50% last year to 66% in 2017. These findings may point to greater maturity in security solutions among US companies, with threats being seamlessly detected and mitigated before requiring C-level attention.

**AT LEAST HALF OF COMPANIES PREFER IN-HOUSE SECURITY MANAGEMENT**

When it comes to managing security, all organizations have the same fundamental options: manage internally, rely on an ISP or carrier or outsource to a security provider. Around the world, at least half of the companies surveyed prefer to manage security internally with their own team. About one-third prefer to rely on their ISP or carrier, while 14% opt for management by a dedicated security provider. In Europe, there is a stronger preference to rely on ISPs and carriers (cited by 39% versus 26% in the US), while US companies lean more on dedicated security vendors (cited by 19% versus 10% in Europe).

**AUTOMATION TAKES A SEAT IN THE BOARDROOM**

Four in five executives reported having already or recently implemented more reliance on automated security solutions. Around the globe, two in five indicated that within two years, automated security systems—such as machine learning and artificial intelligence (AI)—will be the primary resources to maintain cyber security. That sentiment was more widely expressed among European executives.

The survey also probed executives on whom they trust more: humans or machines. One-third of execs trust automated systems more than humans to protect their organization. Twenty-five percent trust humans more, and another quarter trust both equally. The remainder say that both have their vulnerabilities; they trust neither more than the other. These perceptions of trust were consistent across regions.

**PRIVACY OR PROFIT? EXECUTIVES SUPPORT GREATER GOVERNMENT INTERVENTION**

The survey used a 10-point scale, with 10 being the highest, to understand executives’ views on how well current regulations address real security issues for them as individuals and as corporate leaders. Overall, respondents rated regulations a 6.8 for personal and 6.9 for corporate. European executives scored laws a bit higher at 7.3 for both personal and corporate.

Despite that relatively positive outlook, two-thirds agree that privacy is compromised by current laws related to information security. Further, 79% think the government should do more to protect consumers’ personal information—and that is true even among those conceding that more stringent legislation could adversely affect their day-to-day operations.

A noteworthy finding among UK execs: More than half reported that they are more concerned about cyber security than Brexit.
C-suite executives are leading organizations in an era of fast-paced digital transformation and shifting regulatory landscapes. Radware wanted to understand how executives view cyber security and how their organizations are managing and purchasing security solutions. What follows is a summary of the global findings—as well as analysis of noteworthy differences by country or region.

**CYBER SECURITY: A KEY PRIORITY ACROSS THE BOARD**

The majority of respondents (85%) said that security threats are a CEO or board-level concern in their company. The numbers skewed a bit higher in Europe (particularly in the UK), where 90% of respondents said security is now a top-level concern. Among all respondents, 95% told us that security is an extremely or very important priority. About three in five (62%) rate it “extremely important,” marking a slight increase from last year, when just 53% did so. In the US, ratings of importance are unchanged since 2016, but in Europe, the “extremely important” rating increased from 50% last year to 66% in 2017.
A noteworthy finding among UK execs: Half reported that they are more concerned about cyber security than Brexit. One-third are more concerned about Brexit, and the rest are equally as concerned about both.

We asked respondents how the importance of cyber security has changed, if at all, in the past year. Globally, four in five say it has increased in importance. Half of Europe (49%) reported a significant increase; in the US, half (51%) indicated a moderate increase.

**PREVALENCE OF CYBER-ATTACKS: PERCEPTION VS. REALITY**

Consistent with the 2016 survey findings, close to three in five executives (56%) indicated that their company had experienced a cyber-attack in the past 12 months. Globally, about 30% experienced one such attack, and another third had two or three attacks. In the US, more than one-fourth reported 11 or more attacks. The frequency of attacks varied, with half saying they were targeted quarterly or annually. In the UK, one-third of respondents reported being attacked weekly.

In this year’s survey, European executives were more likely to report an attack than their American counterparts (75% vs. 36%). Does this mean European businesses are under cyber siege? No. In fact, Radware’s security industry survey has not shown evidence of significant regional difference in quantities of cyber-attacks—with 98% of frontline security teams globally reporting experiencing at least one attack in 2016. Cyber security was already top of mind in the US. We believe this new finding suggests that cyber security is now gaining even greater visibility—and becoming an even higher priority—among European executives.

There are numerous plausible reasons for the discrepancy between what security teams and C-suite executives are reporting in Radware’s respective surveys. Radware believes the discrepancy can be explained by these factors:

- **Culture.** US-based cyber-security teams seem less apt to communicate with execs about what they view as “non-events”—that is, incidents that they successfully mitigated. As a result, US executives could be hearing about only big, noteworthy incidents. In Europe, cyber-security teams appear to feel a greater obligation to be transparent with executives.
Preparedness. Radware experience suggests that US-based security infrastructures are generally more mature than their counterparts in Europe. That could lead to more proactive, automated threat detection and mitigation for the vast majority of low-level attacks, obviating the need for C-suite reporting. In addition, as European companies work to bolster their defenses, security teams are likely working hard to justify requests for larger cyber-security budgets. Keeping the C-suite apprised of every incident, large or small, helps create a greater sense of urgency.

Regulations and internal procedures. Overall, European companies operate under much stricter regulations in terms of information security and data privacy. These requirements may encourage more frequent and comprehensive reporting than is the norm in the US, where the regulatory environment appears to be shifting to fewer, not more, data privacy protections (more on that later in the report).

MOST-FEARED CYBER-ATTACKS AND BUSINESS IMPACTS

When it comes to cyber-attacks, three in five executives claim that malware, bots or ransomware attacks would be extremely or very detrimental to their business. Globally, more than half of executives indicated that other threats would also be detrimental. Among them: web application attacks (55%), distributed denial-of-service (54%), advanced persistent threats (54%) and socially engineered threats (52%).

RESULTS BY REGION

In Europe, executives cited malware and bots (66%), ransomware (62%) and advanced persistent threats (61%) as the top-three most detrimental threats. UK executives expressed greater concern about advanced persistent threats than did their peers in other regions.

In the US, executives pointed to malware and bots (58%) and distributed denial of service (DDoS) (54%) as the top two most detrimental cyber-attacks.

Radware’s global survey also affirms that executives no longer view cyber threats as discrete, technology-related risks. The C-suite now understands that cyber threats are business threats that can undermine their ability to operate and to compete successfully. In particular, executives are concerned about potential impacts of security threats, including negative customer experience (cited by 39% of respondents), as well as losses to a company’s brand reputation (36%) and revenue (34%). That marks a slight change from last year’s survey, when executives reported being most concerned about brand reputation loss (34%), operational loss (31%) and revenue loss (30%).

RANSOM ATTACKS: REPORTED DECLINE

Overall, most of this year’s respondents have not experienced a ransom attack in the last year. Globally, just 12% reported being the victim of such an attack. Regionally, there were significant differences. Sixteen percent of US executives reported experiencing ransom attacks in our 2016 survey; this year, the number fell to just 6%. Last year, 12% of UK executives reported experiencing ransom attacks. In this year’s survey, 23% of UK executives reported having a ransom attack. Across all three European countries, 18% reported ransom attacks, with the UK and Germany particularly hard hit.
As with our findings on all types of cyber-attacks, there could be cultural and/or regulatory explanations for these differences. With EU countries bracing to meet the stringent requirements of the General Data Protection Regulation (GDPR), their security teams may be more likely to communicate about ransom attacks. In the US—where the current climate is one of rolling back regulations and consumer protections—security teams may feel less pressure to be transparent with the C-suite.

We also wanted to know how executives would respond if they were to experience a ransom attack. In the 2016 survey, 77% of US and 91% of UK executives who had not experienced a ransom situation said they would not pay their attackers. Among those who actually had experienced a ransom attack—especially in the UK—the numbers were different. Last year, 64% of UK executives reported paying up, while 29% did so in the US.

This year’s findings are similar but slightly more moderate. Among those who have not experienced a ransom situation, 46% said they would not pay, with about three in ten indicating it would depend on the risk, a new option this year. Among the few respondents who have experienced a ransom attack, none in the US paid. The eight in Europe who paid the ransom were evenly split between the UK and Germany, with four paying less than €5,000 and four paying €5,000 or more.²

**RESULTS BY REGION**

In the US, just 6% of executives reported that their company was targeted by a ransom attack.

In Europe, the rate of ransom attacks was 18%—three times that of the US. The UK and Germany were particularly hard hit (23% and 19%, respectively), while France had a relatively lower incidence of ransom attacks (12%).

**THE WANNACRY RANSOM CAMPAIGN**

After conducting the executive survey, attackers launched The WannaCry ransom campaign, a worldwide extortion campaign that hit dozens of organizations across the globe. Among them: Chinese universities, Russia’s Ministry of Internal Affairs and the UK’s National Health Service, as well as such enterprises as Federal Express, Telefonica and Renault.

This attack spread by leveraging recently disclosed vulnerabilities in Microsoft’s network file sharing SMB protocol (CVE-2017-0144 – MS17-010i), which were leaked in exploit kits EternalBlue and DoublePulsar. The attack targeted computers that were not updated properly.

This attack reinforces the learnings from Radware’s 2016-17 Global Application & Network Security Report, which indicates that crime—ransom in particular—was the top motivation for cyber-attacks in 2016. While we may have seen a lull in ransom activity, once criminals had a vehicle to extort money from organizations, they immediately leveraged it and ran a massive, global ransom campaign.

---

² For more insights about cyber ransom, see Radware’s publication, *Cyber Ransom Survival Guide: The Growing Threat of Ransomware and RDoS – and What to Do About It.*
This year’s survey respondents affirmed that their organizations are actively integrating digital technologies—and that cyber security is the number-one driver of their digital transformation. With nearly half of all executives (47%) cited improving information security as a major goal of their digital transformation. What’s more, for three-quarters of organizations, cyber-security considerations were critical in shaping decisions to transform aspects of the business to digital. Cyber-security considerations weighed more heavily for European executives, with 88% citing them as very or extremely critical (vs. 61% in the US).

**RESULTS BY REGION**

Overall, almost half of executives (47%) cited improving information security as a top-three goal of their digital transformation.

In Europe, information security is the top goal (47%). Business efficiency ranked second (34%), followed by reducing operational expenses and improved competitive advantage (both 28%).

- **UK** – information security (47%), business efficiency and improved competitive advantage (both 34%)
- **France** – information security (49%), improved customer experience (39%), reduced operational expenses (36%)
- **Germany** – information security and business efficiency (47%) and reduced operational expenses (34%). Business efficiency is more of a goal in the US (50%) vs. Europe (34%)

In the US, business efficiency surpassed improved security as the number-one priority (50% versus 47%), with reducing operational expenses (38%) rounding out the top-three goals of digital transformation.
Companies are not just digitizing their operations; a growing number are also automating their security. Security automation has been a growing trend in recent years. It’s a case of fighting fire with fire: As threats have become incredibly dynamic, detection and mitigation solutions have risen to the challenge with their own increases in automation and adaptability.

Consider the rise of IoT bots and botnets. Once a futuristic-sounding threat, these methods of attack have proved to be lethal. The year 2016 brought attacks on Krebs, OVH and Dyn by the IoT botnet known as Mirai. While Mirai was neither the first nor the most sophisticated IoT botnet, it was highly effective in taking down its targets. These attacks represented a milestone in IoT botnet and DDoS history—and served as a wake-up call to anyone responsible for safeguarding networks, systems and data.

This year’s executive survey supports the assertion that security automation has now reached an inflection point—with about four in five of the executives reported having already or recently implemented more reliance on automated solutions.

A significant portion of executives foresee automation as the wave of the not-so-distant future. Overall, 38% indicated that automated security systems—such as machine learning and AI—will be the primary resource for maintaining cyber security within the next two years. In Europe, nearly half of executives (46%) expressed this view. In that same time period, about one-quarter of all executives expect to rely on an even mix of people and machines to maintain cyber and network security. That propensity is nearly the same in the US (27%) versus Europe (21%). The 2016-2017 Global Application & Network Security Report featured an op-ed by the CISO of a top-five US carrier, who wrote:

“Attacks and techniques change daily. You need flexible solutions and the ability to make adjustments just as frequently to protect the business. Pull those levers to keep pace with ever-changing threats to your applications and networks.”

Radware’s research also point to a perceptional shift among C-suite executives—who seem to be warming to the idea of security supported by AI, machine learning and other forms of automation. In the survey one-third of executives reported trusting automated systems more than humans. Twenty-four percent said they trust humans more, and the same percentage said they trust people and machines equally. The remainder? They told us that both have vulnerabilities, so they trust neither.
HACKERS: TO HIRE OR NOT TO HIRE

This year’s survey also revealed that European executives are more likely to report willingness to hire ex-hackers as part of their security team. In Europe, 58% said they were very or extremely likely to do so, while just 27% of US executives expressed that willingness. Fully one-quarter of US executives said that their company was not very likely and 36% said their organization was somewhat likely to hire former hackers.

Among European executives, engaging ex-hackers is not just a hypothetical question; it is already common practice. Nearly half of respondents in Europe have already invited hackers to test their systems for vulnerabilities. That’s significantly higher than in the US, where only 31% of executives say their companies have engaged hackers for vulnerability testing.

Globally, those who already have hired hackers or are open to this practice would let hackers test the effectiveness of existing network systems, network infrastructure and databases (see Figure 3).

What is behind Europeans’ propensity to work with ex-hackers? Radware believes it could be rooted in a perception that hackers are more likely to be agile and creative in identifying vulnerabilities. For starters, most hackers don’t complete formal studies in computer engineering. Nor do they participate in security training programs that adhere to a certain methodology. They think outside the proverbial box and can therefore help with vulnerability mapping and forensics. Further, hackers tend to share information and openly discuss offensive tools and tactics. Most organizations don’t or do so to a much lesser extent.

It may also be that Europeans companies are adhering to the philosophy of “Keep your friends close and your enemies closer.”

At Radware, we have hired former white-hat hackers, who continue to contribute valuable experience and perspective to our team.

RESULTS BY REGION

In Europe, 78% of executives expressed willingness to hire ex-hackers as part of their internal security team. Only 31% said their organization would be not very or not at all likely to do so. In France, 82% of executives said their companies would be somewhat, very or extremely likely to hire ex-hackers, compared to 78% in Germany and 74% in the UK.

In the US, 63% of executives said their organizations would be somewhat, very or extremely likely to hire ex-hackers; 35% said they were not very or not at all likely to make these hires.
C-SUITE PRIORITIES: PRIVACY OR PROFIT?

In this year’s executive survey, Radware wanted to gauge executives’ views on privacy—both as individual consumers and as business leaders. While most respondents agree that privacy is compromised by current laws and legislation related to information security, 80% feel the government should do more to protect personal information. That was true whether they were responding as business leaders or as individual citizens—and regardless of their home country.

EUROPE: COMMITTED TO PRIVACY

Since the mid-1990s, legislation that protects the information privacy of individuals in the EU is primarily based on EU Directive 95/46/EC: the Data Protection Directive. This legislative act set out minimum standards on data protection—offering guiding principles without specific instructions or harsh penalties for non-compliance. Each country within the EU has taken Directive 95/46/EC and transposed it into its own, local data protection laws.

Figure 4. Is privacy compromised by current laws?
In January 2012, the European Commission proposed a comprehensive reform of the data protection rules in the EU. Known as GDPR, it is the largest reform in data protection law in the past 20 years. The goal: to return control over personal data to EU citizens and simplify the regulatory environment for business through greater cross-EU consistency.

Slated to take effect on May 25, 2018, GDPR aims to provide protection concerning the processing of personal data and the free movement of such data. It represents an entirely new set of regulatory rules and measures to comply with and implement by any organization that controls or processes any form of personal data. Under the GDPR, “personal data” is to be interpreted in the wide sense of the term—and pertains to any information relating to an individual, whether his or her private, professional or public life. Personal data can include anything from a name, picture, email address, financial details, posts on social networks or even a computer’s IP address.

Not abiding with the GDPR will be met with enforced action including fines of up to €20 million or 4% of the offending organization’s annual worldwide revenue when facing a breach of the data protection rules. The GDPR includes provisions that promote accountability and governance that can be audited with non-compliance, leading to administrative fines of up to €10 million (or 2% of annual worldwide revenue).

Whenever a company wants to trade or do business with one or several of the EU member states, it will have to prove adequacy. In other words, virtually any company that does business in the EU will need data protection standards that are equivalent to the EU’s GDPR starting in May 2018. This virtually makes GDPR a global, worldwide regulation affecting organizations and businesses around the globe—and that is poised to have a huge impact on the competitiveness of US companies in EU markets.

In France, companies also face a specific law from 1978, Loi Informatique et Libertés, which strictly supervises the use of personal data and the consolidation/filing of extensive databases containing personal, private data. For German companies, the shift to the GDPR will likely be less traumatic, as national laws already mandate prompt and thorough reporting by any organization deemed part of “critical infrastructure.” For companies in the UK, the road may be a bit rockier as they face massive uncertainty related to Brexit. Initial signs seem to suggest that most companies will still work to meet GDPR requirements, as those will govern any data that large, UK-based companies may hold in other EU countries.

UNDOING NEW PROTECTIONS IN THE US

At the end of the last presidential administration, the US Federal Communications Commission (FCC) approved a set of rules designed to increase protections for consumer privacy. As explained in an FCC news release, “The rules separate the use and sharing of information into three categories and include clear guidance for both ISPs and customers about the transparency, choice and security requirements for customers’ personal information.

- **Opt-in:** ISPs are required to obtain affirmative ‘opt-in’ consent from consumers to use and share sensitive information. The rules specify categories of information that are considered sensitive, which include precise geo-location, financial information, health information, children’s information, social security numbers, web browsing history, app usage history and the content of communications.

- **Opt-out:** ISPs would be allowed to use and share non-sensitive information unless a customer ‘opts-out.’ All other individually identifiable customer information – for example, email address or service tier information – would be considered non-sensitive and the use and sharing of that information would be subject to opt-out consent, consistent with consumer expectations.

- **Exceptions to consent requirements:** Customer consent is inferred for certain purposes specified in the statute, including the provision of broadband service or billing and collection. For the use of this information, no additional customer consent is required beyond the creation of the customer-ISP relationship.”

Before the FCC could actually enact those rules, however, the then-newly elected presidential administration rolled them back—signaling the US’s shift away from Europe in terms of privacy laws. In a similar signal of deregulation, on May 18, 2017, the FCC voted to begin repealing what are commonly referred to as “net neutrality” laws. “[Net neutrality is] the idea that phone and cable companies should treat all of the traffic on their networks equally—no blocking or slowing their competitors, and no fast lanes for companies that can pay more,” as an NPR article succinctly explained. Enacted in 2015, these rules had placed ISPs under strict FCC oversight. Now it appears that the FCC will be taking a lighter touch in regulating phone and cable companies, potentially easing the regulatory burden for business but creating more privacy risks for consumers.

THE PRIVACY PENDULUM

While the EU and, in all likelihood, the post-Brexit UK, are tightening the reins on consumer privacy protections, the US seems to be headed in the opposite direction. How these competing forces will affect cyber security—and global competitiveness—remain to be seen.

RESULTS BY REGION

In Europe, 67% of executives agree that privacy is compromised by current privacy laws and legislation related to information security.

61% OF EXECUTIVES IN FRANCE

63% OF EXECUTIVES IN GERMANY

77% OF EXECUTIVES IN THE UK

Across the European countries, 83% of executives said that government should do more to protect privacy.

94% GERMANY

76% FRANCE

80% UK

In the US, the finding was similar, with 66% indicating that current laws are putting privacy at risk and 75% looking to government to do more.

MANAGING SECURITY: IN, OUT AND IN-BETWEEN

Given the complex challenges of digital transformation, changing regulatory landscapes, highly dynamic cyber threats—and equally adaptive security solutions—how are companies around the world managing cyber security? Do they prefer do-it-themselves security or support from their ISP/carrier or services through a dedicated security partner? How do those preferences vary by region of the world?

Globally, more than half of the executives surveyed reported a preference for managing cyber security internally. About one-third (32%) say they count on a security provider (such as their ISP or carrier), while 14% lean on a dedicated security vendor.

RESULTS BY REGION

In Europe, 51% of companies manage security within their own organization. UK companies are particularly keen on internal management (71% compared to 33% in France and 47% in Germany). Across all three European countries, 49% opt either for management by their ISP/carrier (39%) or management by a dedicated security provider (10%). Interestingly, companies in France are most likely to opt for third-party management (cited by 55% of executives).

In the US, more than half of companies (54%) manage their own security. A smaller share (26%) lean on their ISP or carrier, while a comparatively larger percentage (19%) count on a dedicated security vendor.
After probing executives on the composition of their security teams, we found that most rely either on proven technical talents within their organization (42%) or third-party experts with long track records in IT (36%). Just 5% count on white-hat hackers, while 12% use some combination of all three types of resources. Compared to just 1% of European companies, about one in ten US corporations has no in-house security team.

EVALUATING APPROACHES TO SECURITY MANAGEMENT

What is the “right” approach? As the diverse responses suggest, each organization must find the optimal answer for its risks and needs. Each approach has advantages and disadvantages that must be weighed in the larger context of an organization’s strategy, structure and depth and breadth of cyber-security resources.

INTERNAL SECURITY MANAGEMENT

Organizations that decide to manage their own security are often drawn to the high level of control and the ability to make policy adjustments very quickly. An organization should have a deep understanding of its own network and application behavior—as well as the business’s processes and needs. As with virtually any in-house solution, an organization can then implement a high level of customization to secure its network and applications. This security approach can also help simplify management, with no confidential data leaving the network, and faster return-on-investment calculation. When exploring this type of approach, consider the following:

- Can the organization make the necessary investments in obtaining and maintaining security expertise?
- Do the organization have sufficient resources and knowledge not only to operate the security solutions but also to stay on top of new and emerging threats?
- Since most IT infrastructures combine on-premise and cloud-based systems, in-house management require a patchwork of security solutions. Is the organization prepared for the burden of managing multiple solutions?
- How will the organization ensure that its approach is continuously adaptive? Without capabilities, such as machine learning, virtually any in-house security solution is obsolete as soon as it is deployed.
COUNTING ON A CARRIER OR ISP
Relying on a carrier, Internet or cloud service provider is another popular approach to managing security. Companies may gravitate to this option because the ISP or carrier may be local—that is, in the same time zone and with no language barriers. They may have long-standing relationships with their carriers that include a certain level of trust. Engaging a carrier, ISP or CSP may also help reduce the risk of relying too heavily on in-house talent, which can be difficult to retain. Above all, businesses are drawn to a security partner as a “worry-free” way to manage security. When evaluating this approach, consider the following:

- How sophisticated is the ISP/carrier’s security infrastructure? Can it keep the organization up and running even during a large or complex attack? Will it offer the organization a mitigation service, or does it “blackhole” or cut off all traffic while under attack? Make sure to understand how this practice might inadvertently affect multiple customers’ systems.

- How well does the ISP/carrier know the organization’s applications? Without a detailed understanding, it may not be able to protect against DDoS attacks.

- How many organizations is the ISP/carrier supporting, and how can each organization be certain it will receive the support it needs?

SECURING DEDICATED—AND SPECIALIZED—EXPERTISE
A third option: engaging a specialized security vendor to manage security across on-premise and cloud solutions. Similar to using an ISP or carrier, counting on a specialized vendor removes dependence on in-house talent. It’s also comparatively “worry free.” Beyond that, businesses typically opt for this approach because they want a vendor that stays on the leading edge of new and emerging threats—and offers a full portfolio of continuously adaptive solutions to detect and mitigate attacks. It is a classic argument to focus on one’s core business—and leave specialized functions to experts who focus on those. When exploring a specialized security vendor, consider the following:

- Can that vendor protect the organization’s unique network infrastructure? If the organization operates with a hybrid network, ensure that the vendor can protect both the organization’s physical and cloud infrastructure versus having to look for different solutions that do not deliver complete visibility across the entire network’s security.

- Will the vendor offer the organization a “personal” connection? Will they take the time to understand the organization’s system architecture and provide a solution and payment structure that meets the organization’s needs?

- What are the regulatory considerations? Does the organization face a mandate not to move its data out of the country?

These considerations can help any organization as it navigates increasingly complex and fast-changing security threats. As this research from Radware shows, cyber security is top of mind for executives around the globe. Effective security management is, and will continue be, a key C-suite priority.

ABOUT THE RESEARCH
On behalf of Radware, Merrill Research surveyed 200 executives—100 in the US and 100 in Europe in April 2017. To participate in the 2017 Executive Application & Network Security respondents were required to be at company with at least $250 million (or equivalent) in revenue and hold a title of senior vice president level or higher. By design, the survey required at least half respondents to be C-level executives, though this year’s research attracted far more top-ranking corporate leaders. About half of the companies in the survey have 1,000 to 9,999 employees, averaging about 4,600. US respondents included a few more companies with less than 1,000 employees, but no other significant differences in terms of number of employees.
ABOUT RADWARE

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware’s solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.

LEARN MORE

To learn more about how Radware’s integrated application delivery & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.