radware

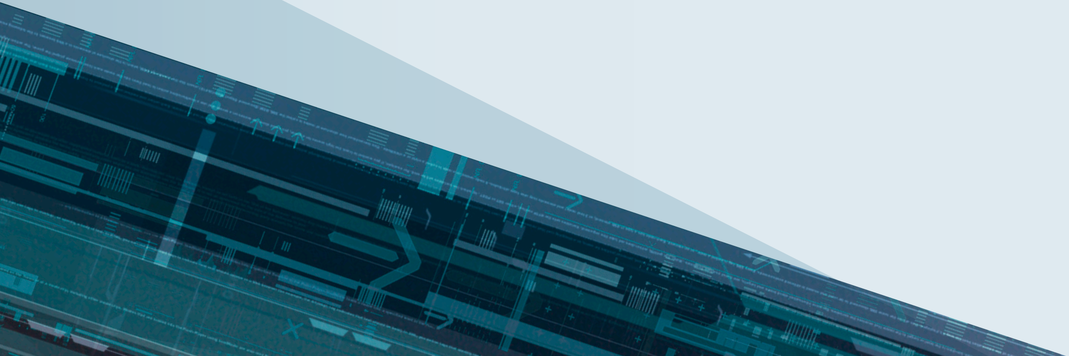
C-SUITE PERSPECTIVES

Trends in the Cyberattack Landscape, Security Threats and Business Impacts

2018

EXECUTIVE APPLICATION & NETWORK SECURITY REPORT

Table of Contents



To compete effectively in today's digital world, corporations rely on their networks to connect with customers and enable business processes.

As more transactions move to the cloud, keeping corporate and customer data safe is a high-stakes endeavor. To better understand how C-suite executives view cybersecurity and their organizations' preparedness to defend against attacks, Radware sought the opinions of senior leaders from the Americas (AMER), Europe and the Middle East (EMEA) and Asia-Pacific (APAC) in April 2018. What follows is a summary of the global cybersecurity trends that are top of mind for senior executives.

Executive Summary

Annually, Radware publishes the findings and analysis from a survey of senior executives globally, with the purpose of better understanding C-suite perceptions of current cybersecurity challenges and opportunities.

This research is designed to help the security community better understand the cyberattack landscape, emerging threats, levels of preparedness and resulting business impacts. It reveals important global trends about the effect that security threats have on how corporations transform their networks and protect the customer experience, as well as intriguing insights into senior executives' main security concerns.

KEY FINDINGS

THE FOCUS ON CYBERSECURITY GROWS AS NETWORKS BECOME MORE COMPLEX

C-suite executives understand that, to transform their businesses, they must embrace the integration of new technologies. Respondents ranked improvement of information security and business efficiency as their main goals. More than 90% of executives reported using multiple public and private cloud environments, with the vast majority of respondents concerned about the security vulnerabilities that this dispersed architecture introduces.

Globally, executives indicated they are ready to embrace automated processes as part of their security protocols. Over the past two years, our research reveals a shift of network security budgets toward technologies that employ machine learning and automation, but manual processes still remain a sizable part of policy enforcement.

SECURING NETWORKS IS CRITICAL TO PROTECTING BRAND REPUTATIONS

Executives are very concerned about the impact that security threats can have on business performance, pointing to the potential loss of customers, brand reputation and operational productivity. Many reported adjusting budget priorities to better secure networks and prevent attacks.

Events that most influence how executives view their companies' security vulnerabilities include high-profile data breaches and nation-state attacks, cyberattacks on their organizations and governmental regulations.

RISK MANAGEMENT CALCULATIONS AFFECT SECURITY INVESTMENTS

C-suite executives face tough choices when deciding where to invest resources to propel their businesses forward. At least four in 10 respondents identified increasing infrastructure complexity, digital transformation plans, integrations of artificial intelligence (AI) and migration to the cloud as events that put pressure on security planning and budget allocation.

C-suite professionals actively monitor what's happening with their networks. Reported instances of ransom attacks jumped dramatically over the past two years. Sixty-nine percent of respondents said that they were hit with ransom attacks, with most paying the ransom. Two-thirds said that hackers can penetrate their networks, and more than half have experienced cyberattacks in the last 12 months. As the demand for security professionals outpaces the supply, executives are increasingly looking to carriers or ISP/CSPs to manage security.

NETWORK SECURITY CONCERNS VARY BY INDUSTRY

The impacts of attacks on corporate networks can vary depending on the industry in which companies compete. Manufacturers that have long embraced automation as a means to boost efficiencies and production reported plans to integrate automation in security measures with a corresponding shift in their IT budgets.

The finance/insurance industry continued its forward-thinking use of technology as a business enabler and reported plans to move operations to the cloud while continuing to focus on digital transformation. The retail/wholesale industry is concentrating on managing the increasing complexity of the IT networks, digital transformation plans and the adoption of Internet of Things (IoT) as a means to better serve customers.

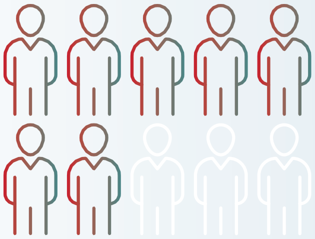
Securing the Digital Transformation

Corporations are continually looking for ways to increase productivity and efficiency. Taking advantage of technology advances in their networks is a proven way to be more agile while reducing costs.

Customers, employees, vendors and partners use mobile applications, chat bots, online portals, email and other tools to interact with brands daily. Every touchpoint adds a layer of complexity to the network that can introduce new, risky attack vulnerabilities.

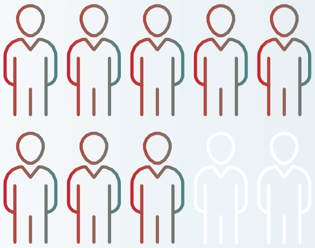
C-suite executives understand that, to transform their businesses, they must embrace the integration of new technologies while at the same time protect data privacy. Respondents ranked improvement of information security and business efficiency as their main goals. Creating a competitive advantage and improving the customer experience closely followed. Half of the executives (47%) also recognized that digital transformation activities place pressure on their organizations' security planning and investment strategy.

PERCENTAGE OF C-SUITE RESPONDENTS WHO ARE GREATLY CONCERNED ABOUT DATA PRIVACY



70%

AMER AND EMEA EXECUTIVES



80%

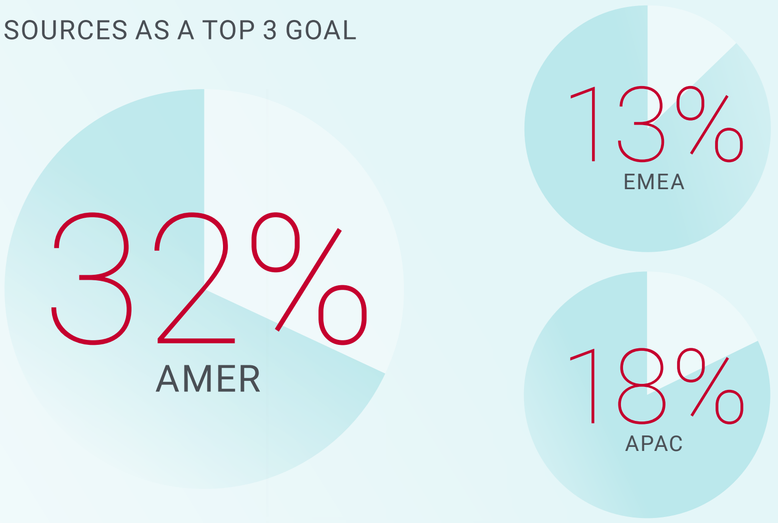
APAC EXECUTIVES

REGIONAL DIFFERENCES: **AMER**

Creation of New Revenue Sources

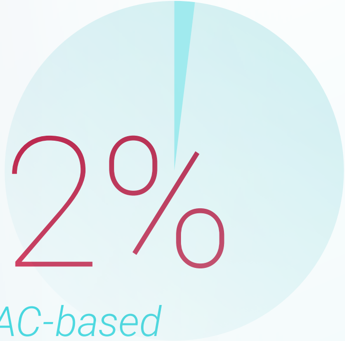
Creating new sources of revenue was more important to AMER respondents versus other regions.

RANKING OF NEW REVENUE SOURCES AS A TOP 3 GOAL



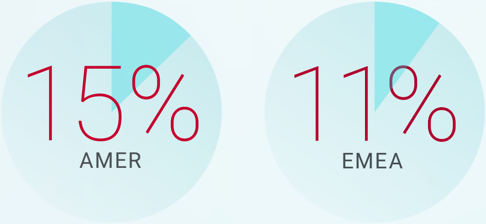
REGIONAL DIFFERENCES: **APAC**

Business Applications in the Cloud



ONLY 2%

of APAC-based companies reported hosting all their business applications in the cloud.



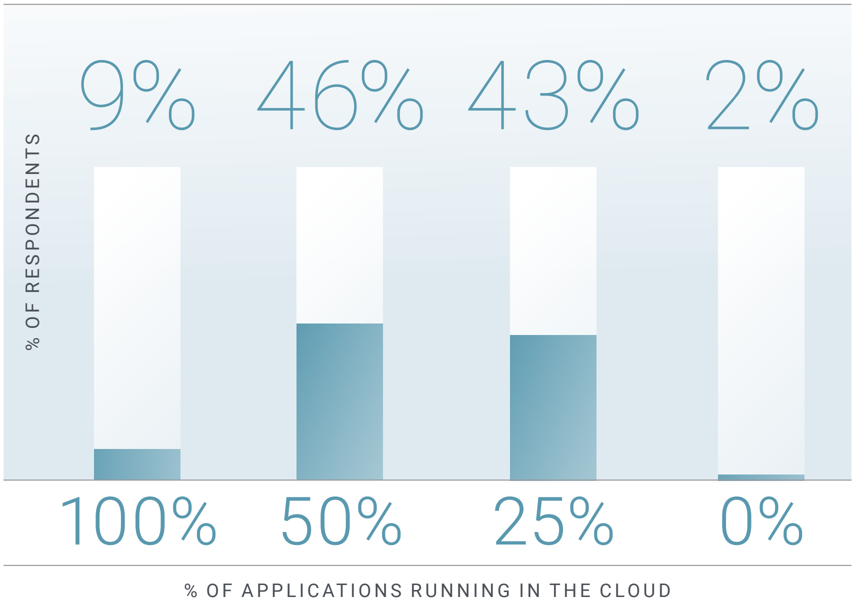
MIGRATION TO MULTIPLE CLOUDS INTRODUCES NEW SECURITY CONCERNS

More than 90% of executives reported using multiple public and private cloud environments as part of their companies' IT infrastructure. Responses indicated that most organizations host 25% to 50% of their business applications in the cloud.

KEY FINDING:

C-suite executives clearly understood that dispersing their network across multiple public and private clouds introduced security risks. The vast majority of respondents (96%) were "very" or "somewhat" concerned about network vulnerabilities.

PERCENTAGE OF BUSINESS APPLICATIONS THAT RUN IN A CLOUD ENVIRONMENT



READY TO TAKE ADVANTAGE OF AUTOMATION

As attack vulnerabilities multiply in increasingly complex networks, over the past two years the majority (71%) of executives reported shifting more of their network security budget into technologies that employ machine learning and automation. About 25% said that the focus of their budgets remained unchanged in this time period.

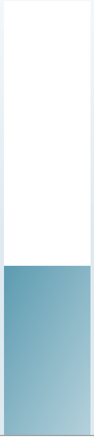
KEY FINDING:

Even though executives said that they were ready to benefit from automated security protections, manual processes are still a sizable part (46%) of policy enforcement, leaving them open to costly human error.

PERCENTAGE OF SECURITY BUDGET ALLOCATED FOR AUTOMATED SECURITY SYSTEMS

39%

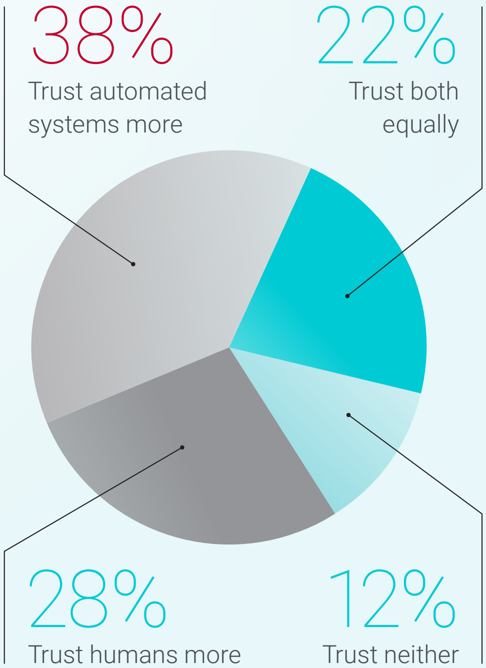
Portion of the security budget across all regions devoted to security systems with automation



REGIONAL DIFFERENCES: **APAC**

Trust Factor

Globally, nearly four in 10 executives trust automated systems more than humans to protect them against cyberattacks.

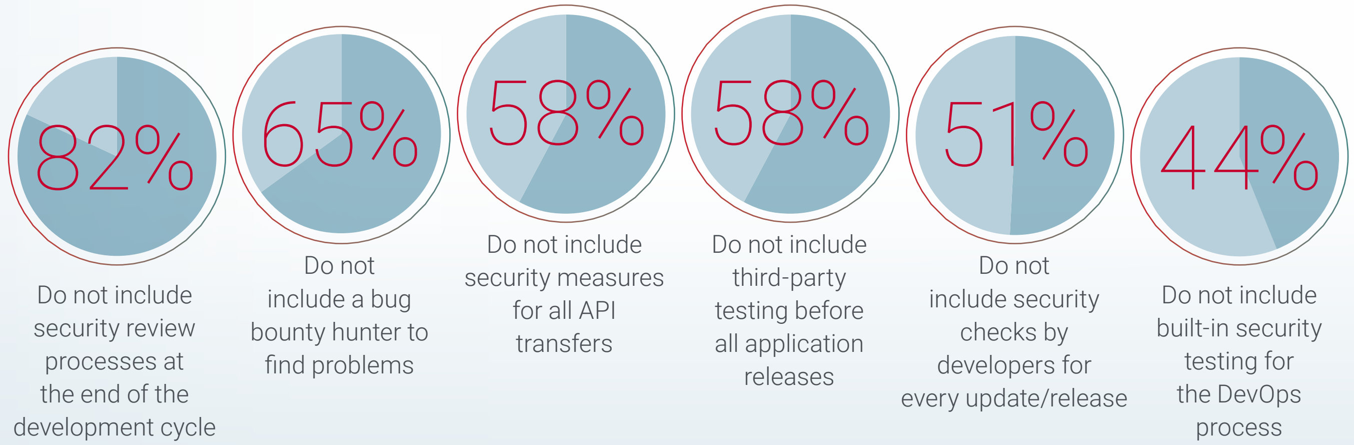


In APAC, more than half of the respondents said that they trusted automated systems more than humans.

DevOps STAND ALONE

In the rush to bring new customer experiences to market, organizations may skip critical security checks, leaving them open to vulnerabilities that could have been mitigated. While some companies have implemented basic security measures, there's a lot left to chance.

EXECUTIVES REPORTED THAT THEY ARE NOT YET INTEGRATING SECURITY PRACTICES INTO THE APPLICATION DEVELOPMENT CYCLE.



Companies that included security as part of their DevOps process reported a **nearly even division between automated and manual policy enforcement**.

UNCERTAINTY ABOUT ENCRYPTED TRAFFIC

As more transactions flood the internet, the volume of encrypted traffic is rising. According to Google's Transparency Report[1], HTTPS encrypted traffic across all platforms (Windows, Android, Chrome, Linux and Mac) has grown about 50% since 2015.

The secure sockets layer (SSL) protocol has been the de facto encryption technology since the early 1990s. Highly publicized vulnerabilities resulted in the development of other protocols such as transport layer security (TLS).

[1] Google Transparency Report: https://bit.ly/2sMEYcr

According to the Radware *2017–2018 Global Application and Network Security Report*[2], 30% of businesses reported suffering an SSL-based attack, with another one in four not certain whether they had experienced such an attack. SSL-based attacks can take many forms, including encrypted SYN Floods, SSL Renegotiation, HTTPS Floods and encrypted web application attacks.

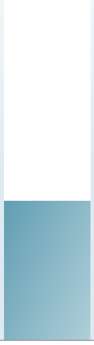
Executives included encrypted attacks on the list of cyberattacks that they viewed as most detrimental. Respondents from AMER (45%) were most likely to cite encrypted attacks as a concern, followed by EMEA (41%).

Many companies operate without protection from encrypted attacks. Part of the challenge they face is that they are unsure about the legalities of decrypting traffic for inspection because of government regulations such as HIPAA and the new GDPR requirements. Many organizations leveraged a WAF and/or ADC to monitor inbound traffic, particularly in AMER (47%).

COMPLIANCE COMPLICATIONS

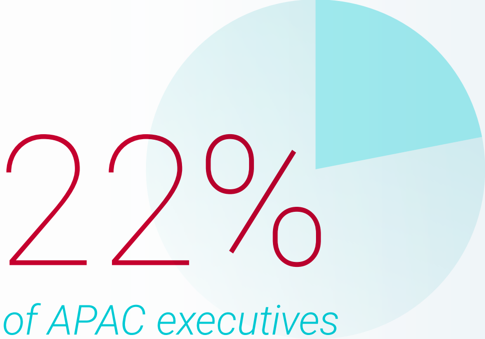
41%

Still reviewing the legalities of decrypting traffic on their networks



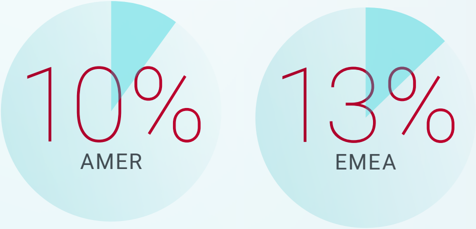
REGIONAL DIFFERENCES: **APAC**

SSL Web Policy



22%

of APAC executives reported that their organizations enforced outbound web policies on web traffic — 9 to 12 percentage points higher than other regions.



10%
AMER

13%
EMEA

[2] Radware *2017–2018 Global Application and Network Security Report*: http://global.radware.com/APAC_2018_ERT_Report_EN

Creating a Secure Climate for Customers

Corporations' networks are the lynchpin of interactions with customers who expect responsive applications, fast performance and, above all, protection of their data.

The foundation of the customer experience is a mix of trust and availability. Organizations' brands take a hit if either factor falters.

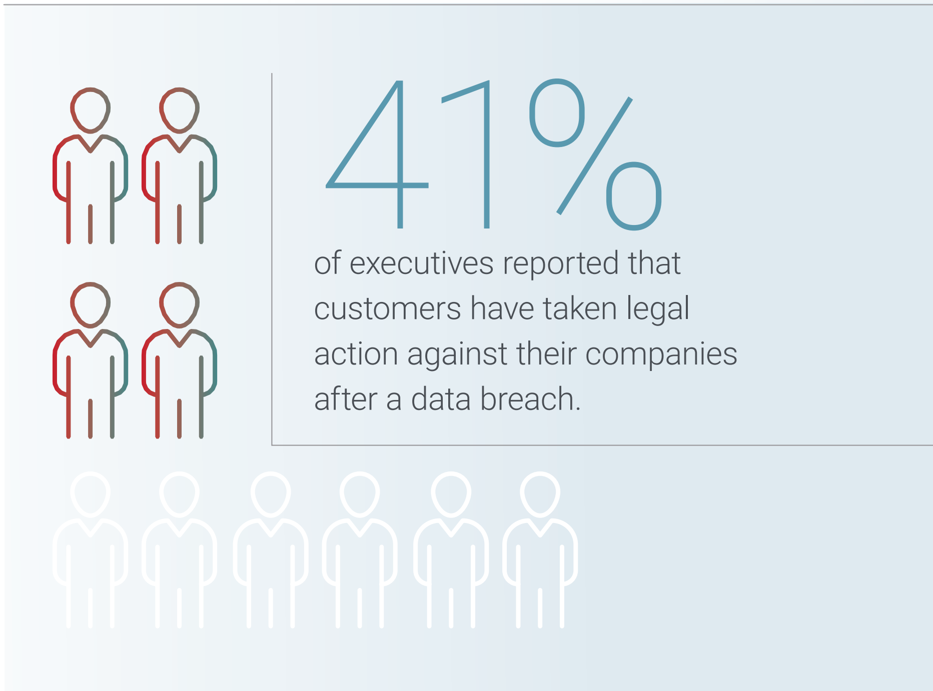
C-suite executives are keenly aware of the effect of security threats on business. Respondents ranked the top three security threats as having the most impact on their business:

1 CUSTOMER LOSS (41%)

2 BRAND REPUTATION LOSS (34%)

3 PRODUCTIVITY/OPERATIONAL LOSS (34%)

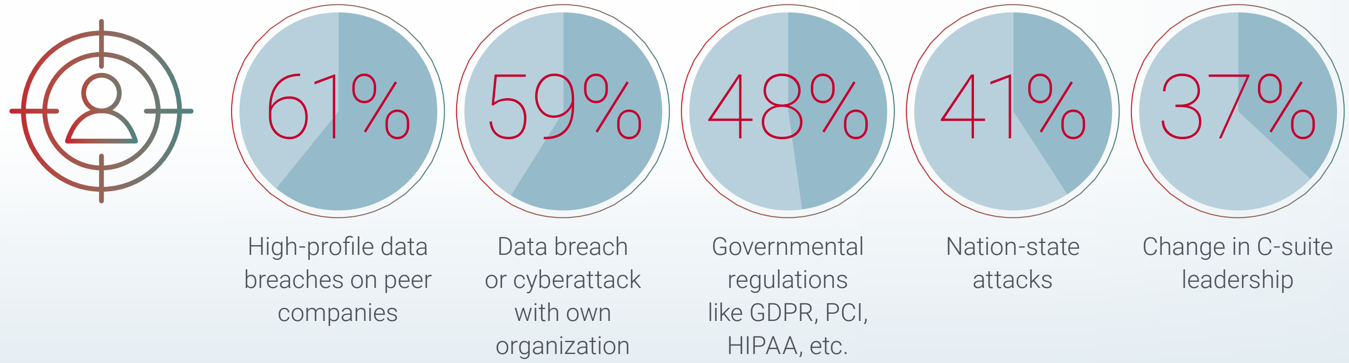
CUSTOMERS FIGHT BACK



TROUBLE IN THE NEIGHBORHOOD

When companies see that organizations in their market have been attacked, they are more likely to make changes to internal security policies.

SPECIFIC EVENTS THAT MOST INFLUENCE CHANGES IN ORGANIZATIONS' SECURITY



High profile data breaches on peer companies are the main influence reported by executives (61%) to evaluate their own security protocols, followed closely by cyberattacks on their own organizations (59%). Executives likely also see that C-suite executives are terminated when data breaches take place at companies like Equifax and Target.

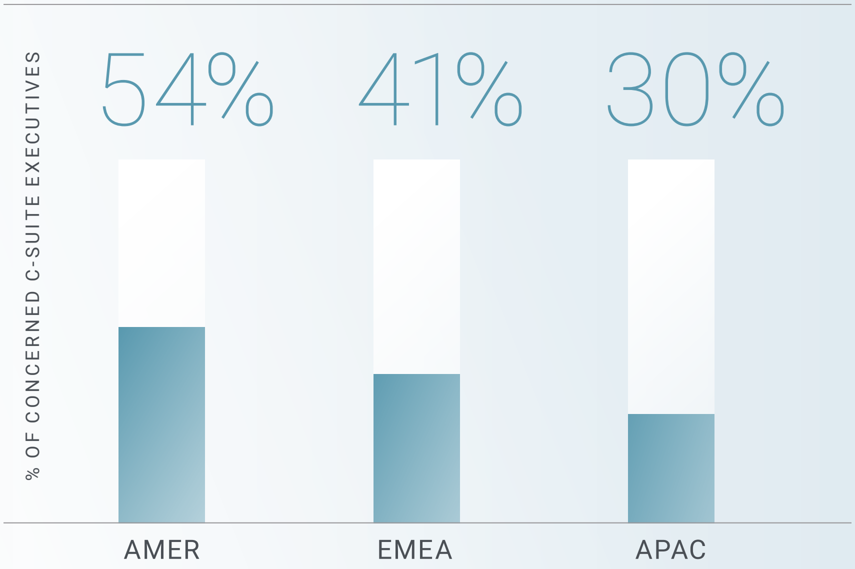
KEY FINDING:

Customers aren't the only victims of cyberattacks. More than four in 10 executives reported that their personal information was exposed as the result of a data breach.

When Nations Attack

Corporate espionage used to be about competing companies trying to steal trade secrets. Now bad actors with a variety of political and military agendas target corporate networks to lift data, make ransom demands or wreak havoc.

C-SUITE EXECUTIVES ARE CONCERNED ABOUT THE POSSIBILITY OF NATION-STATE ATTACKS



Balancing Investments and Risks

C-suite executives face tough choices when deciding where to invest resources to propel their businesses forward.

As the threat of network attacks becomes a question of when, not if, organizations must carefully evaluate the risks associated with security vulnerabilities and the costs of implementing effective security solutions.

40%

of respondents identified the following factors as putting pressure on their organizations' security planning and investment:

1. INCREASING INFRASTRUCTURE COMPLEXITY
2. DIGITAL TRANSFORMATION PLANS
3. INTEGRATION OF ARTIFICIAL INTELLIGENCE INTO BUSINESS PROCESSES
4. MIGRATION TO THE CLOUD

PREPARING FOR THE INEVITABLE

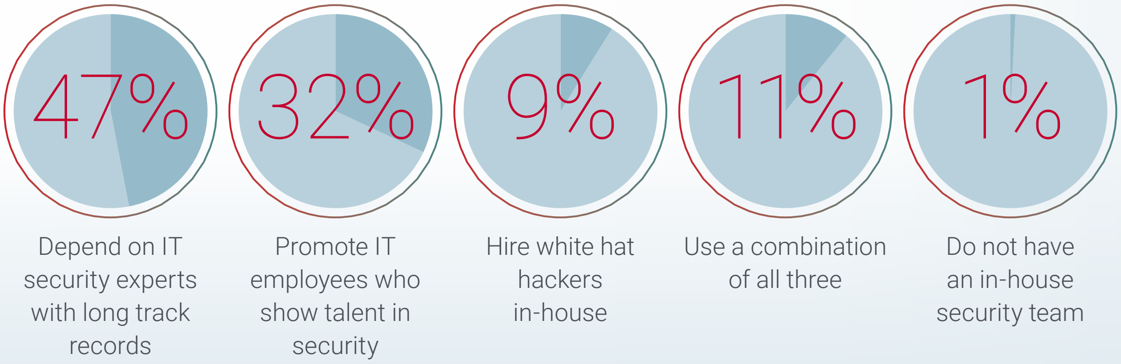
Even though the threat of network attacks hangs over their organizations, about 25% of respondents admitted that they do not have or are in the planning stages of addressing key security concerns, such as performing security assessments on new technology (23%) or working with educational institutions to proactively recruit security specialists (31%).

Security measures that ranked highest as having been in place for more than two years included suppliers being required to fulfill security checks and investment in cybersecurity insurance. Within the past two years, executives reported progress sharing cyberattack intelligence with similar organizations, stricter policies related to working remotely and increased reliance on automated solutions.

KEY FINDING:

Staying abreast of security issues is a never-ending task for C-suite executives. Two in five reported reliance on security vendors to stay current on attack vectors and to maintain updated security measures. About a third of respondents reported that their in-house team managed day-to-day security. About one in five subscribed to a third-party research firm for updates on security issues.

EXECUTIVES DEFINE THEIR INTERNAL SECURITY TEAMS AS COMPRISED OF THE FOLLOWING TALENT TYPES:



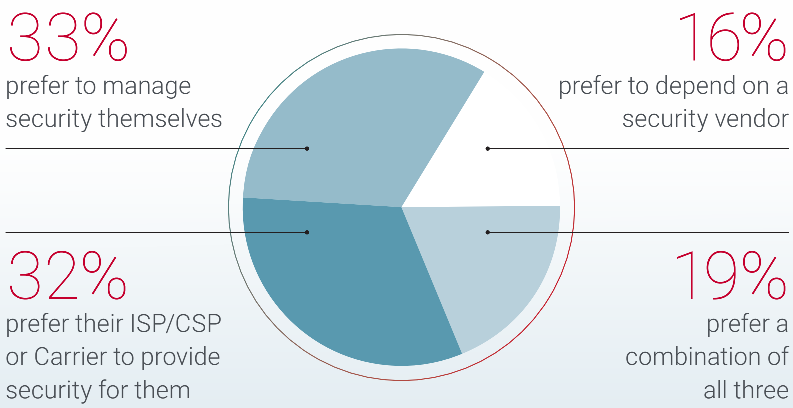
KEY FINDING:
The majority of respondents across all regions (65%–81%) felt that their internal security resources were sufficient to handle their security needs. **Yet 66% believed that hackers could penetrate their networks.**

The internal skills gap is not easily solved because the demand for security professionals outpaces the supply. As a result, more executives reported the need to look to outside security vendors for assistance.

66%

believed that hackers could penetrate their networks.

TALENT SHORTAGES PUSH EXECUTIVES TO TURN OUTSIDE THEIR ORGANIZATIONS FOR SECURITY SUPPORT.



Talent Shortage Ahead

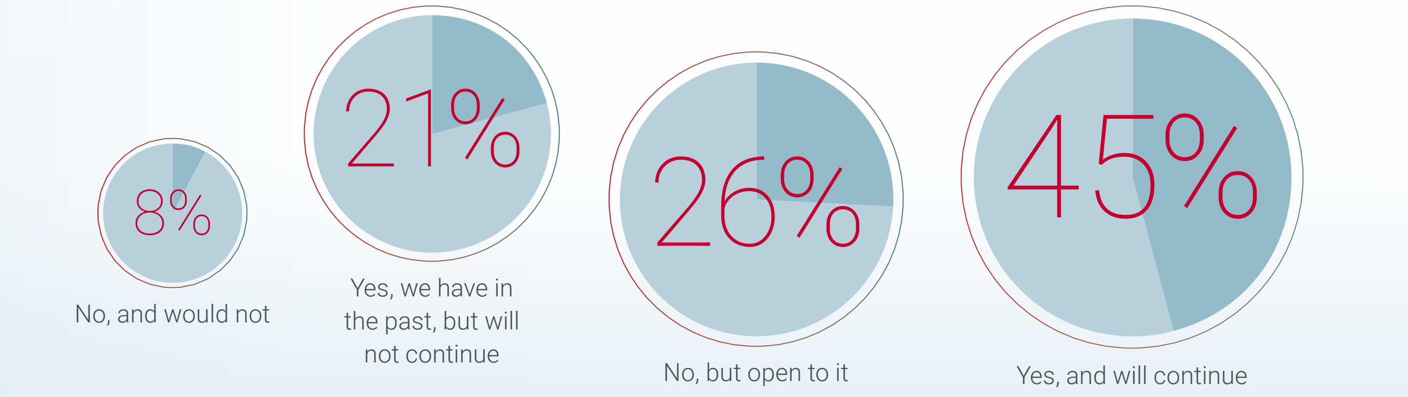
According to a recent Cybersecurity Ventures report[3], by 2021 there will be 3.5 million vacant cybersecurity jobs due to the lack of a pipeline of security talent combined with increasing occurrences of cyberattacks. Competition for knowledgeable staff is likely to increase as demand grows and supply diminishes.

[3] Cybersecurity Ventures press release: https://bit.ly/2Jeq6i9

HIRING HACKERS

About two-thirds of respondents are "extremely" or "very likely" to hire an ex-hacker for their internal security teams, while nearly half indicated that they have already invited hackers to test their systems for vulnerabilities and will continue to do so.

LIKELIHOOD OF HIRING AN EX-HACKER FOR THE IT SECURITY TEAM



There are limits to what executives are open to letting ex- or current hackers test for vulnerabilities, likely because the risk versus reward calculation is too high:

- 15% would never allow hackers to test their Internet of Things (IoT) applications and devices
- 18% would never allow hackers to test their databases
- 17% would never allow hackers to test their policies and procedures

REGIONAL DIFFERENCES: **APAC**

EMEA executives were the first to engage hackers to help secure their networks.

This is likely because networks in those regions are two to three times more likely to be attacked according to the Radware *2017–2018 Global Application and Network Security Report*[4].

In last year's C-suite report, EMEA executives were the most likely to hire ex-hackers for their security teams. This year, AMER and APAC are catching up to EMEA; more than half of all respondents said they were "very" or "extremely likely" to hire ex-hackers.

[4] Radware *2017–2018 Global Application and Network Security Report*: http://global.radware.com/APAC_2018_ERT_Report_EN

TALLYING THE COST OF A BREACH

Data breaches are expensive. Not only do they rack up monetary costs, which directly affect companies' bottom lines, but also and more troubling is the damage inflicted to assets such as brand reputation and customer trust. Almost 40% of respondents estimated the hard cost of every attack to be more than 1 million USD/EUR/GBP/RMB, with cost estimates surging to more than 25 million USD/EUR/GBP/RMB for 5% of respondents. While soft costs are difficult to quantify, it's likely that their impact is much higher over the long run than hard costs.

HARD COSTS

Quantifiable monetary losses from lost business, use of internal resources, cost of external resources, ransom, legal fees and other items that can be accounted for

SOFT COSTS

Qualitative losses, including brand damage, loss of customers, loss of productivity, change in C-suite leadership, drop in stock valuation and other subjective items

EXECUTIVES RANK THE TOP IMPACTS OF DATA BREACHES AND MOST DETRIMENTAL ATTACK TYPES

BUSINESS IMPACTS OF A SECURITY THREAT

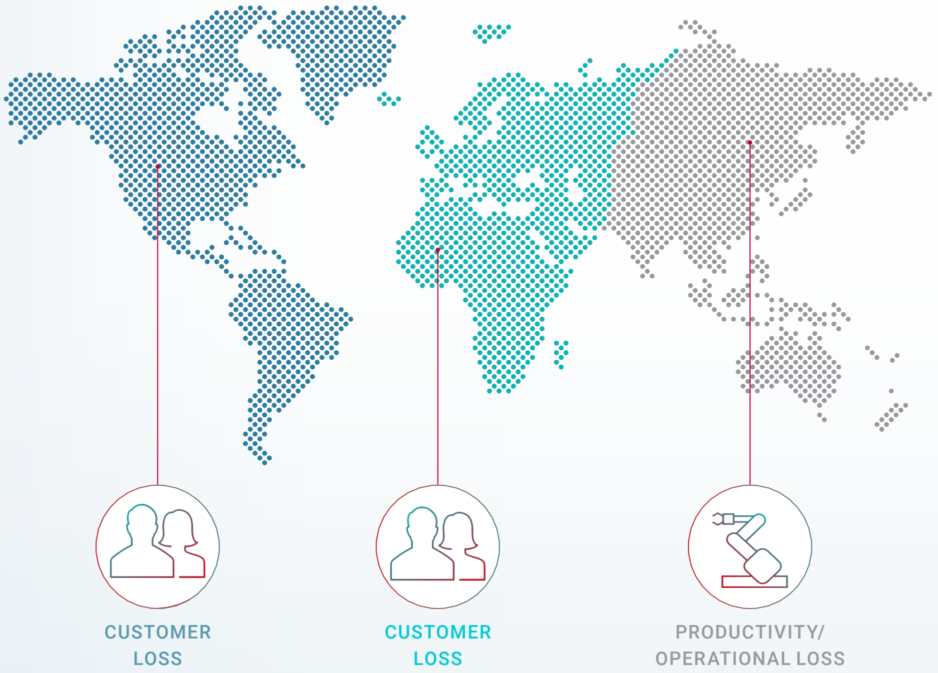
1. Customer loss
2. Loss of brand reputation
3. Productivity/operation loss

MOST DETRIMENTAL ATTACKS

1. Socially engineered threats
2. Ransomware
3. Malware

BUSINESS IMPACTS BY REGION

Respondents from each region placed different weights on the impact of network attacks on their businesses



AMER

1. Customer loss
2. Drop in share price value
3. Revenue loss

EMEA

1. Customer loss
2. Loss of brand reputation
3. Revenue loss

APAC

1. Productivity/operational loss
2. Customer loss
3. Intellectual property loss

CORPORATIONS UNDER SIEGE

The reality is that organizations face a multitude of threats and attacks daily. Many executives do not feel confident that they can prevent hackers from penetrating their networks. They struggle to scale their security infrastructure at the same pace as the technological advances they implement inside their networks.

C-SUITE VIEW OF CURRENT NETWORK THREATS

66%

said that a hacker can penetrate their network

38%

said that their organization was hit with an attack daily or weekly

54%

said that their company had experienced a data breach from one of its mobile applications in the last 18 months

57%

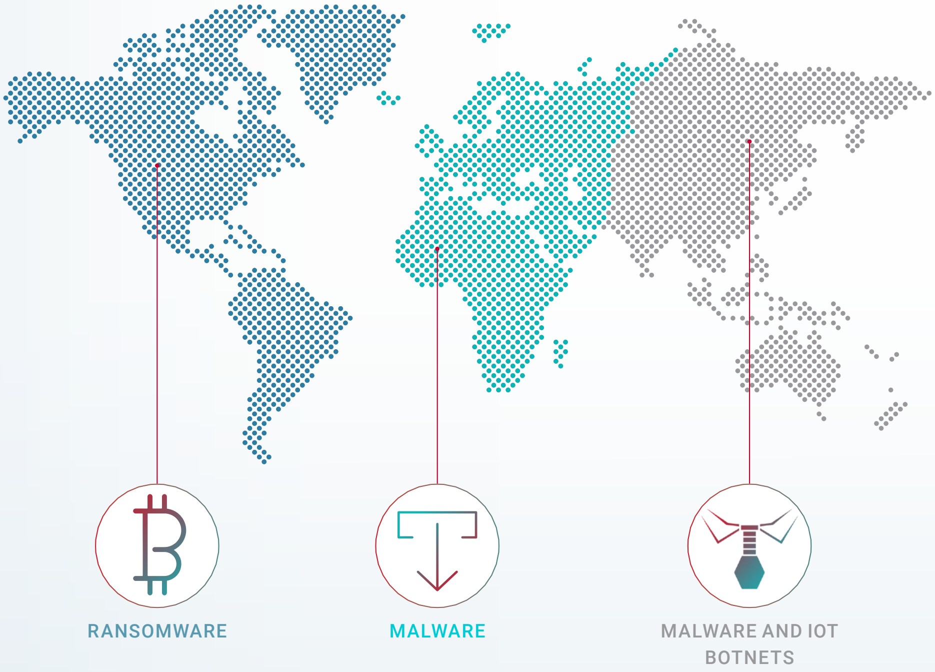
had experienced a cyberattack in the last 12 months

50%

were concerned about the security vulnerabilities created by use of multiple clouds

REGIONAL DIFFERENCES IN ATTACK SEVERITY PERCEPTIONS

Executives identified the following attack types as most dangerous



AMER

1. Ransomware
2. Encrypted
3. Burst

EMEA

1. Malware
2. Advanced persistent
3. Socially engineered

APAC

1. Malware and IoT botnets
2. Socially engineered and web application

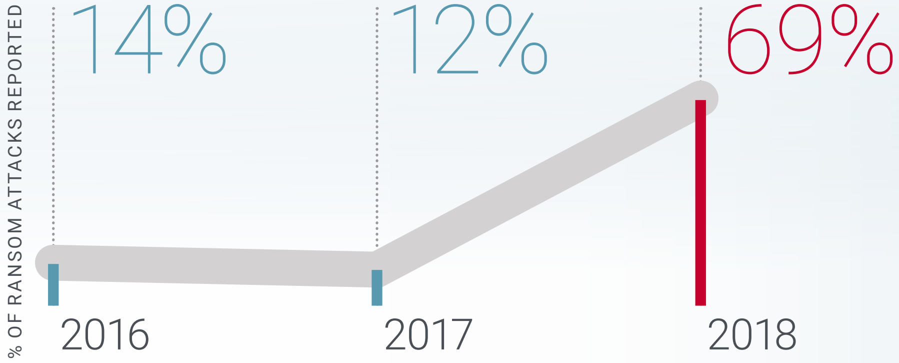
THE RANSOM CALCULATION

Respondents to the annual Radware C-suite survey revealed dramatic growth in the frequency of ransom attacks over the past two years and their organizations' willingness to pay.

RANSOM ATTACKS INCREASED DRAMATICALLY OVER THE PAST TWO YEARS

2/3

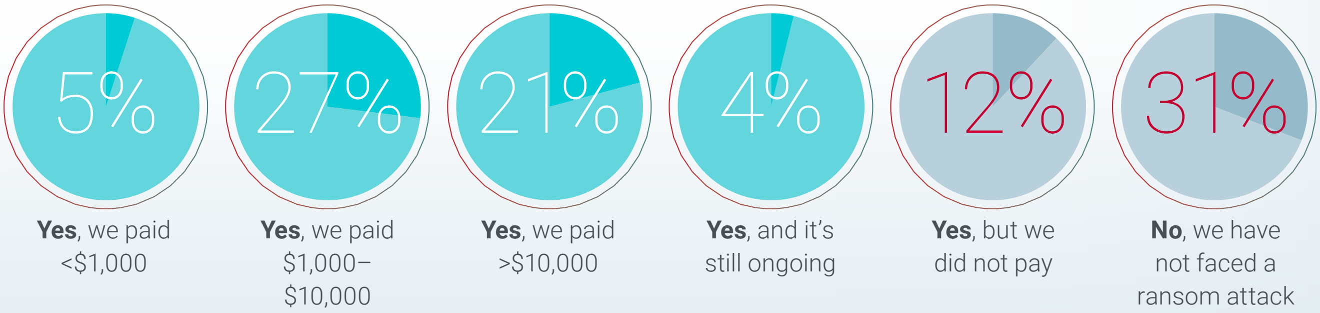
of respondents were victims of ransom attacks



Even though C-suite executives are unlikely to have full visibility into every security threat, the majority (69%) reported that their organizations faced ransom attacks in the past year, with most of those having paid the ransom. Among those who have not experienced a ransom situation, more than half said that they might pay the ransom, depending on the risk or amount.

RANSOM ATTACKS ARE A GROWING CONCERN

Executives reported that their organizations are more likely to have experienced and paid for ransom attacks in the past year than during the previous 12 months.



Impacting Vertical Industries

The impacts of attacks on corporate networks can vary depending on the industry in which companies compete. Directionally, results from respondents in manufacturing, retail and finance reveal emerging security trends specific to the needs of each vertical.

RETAIL/WHOLESALE

Almost two-thirds of retail organizations reported that at least one-half of their business applications are in the cloud and are concerned about security vulnerabilities between cloud networks. The executive suite in this vertical reported almost 20 attacks in the past year. (These are attacks large enough to draw C-suite attention.) This can be troubling because they have the most customer touchpoints on their networks to enable e-commerce.

Executives (77%) said that a data breach within their own organization was the most influential event that affected their own security planning.

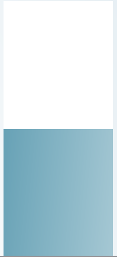
Planning and investment priorities were focused on the increasing complexity of their IT infrastructures (64%), digital transformation plans (58%) and the adoption of IoT (50%).

This vertical was likely (47%) to want a vendor or ISP/CSP to provide security protections.

Executives estimated the cost of an attack at 1.6 million USD/EUR, and two-thirds have paid after a ransom attack.

50%

have been attacked in the past 12 months



MANUFACTURING

Manufacturers have long embraced automation as a means to improve efficiencies and boost production. So it's not surprising that respondents are focused on managing the increasing complexity of their IT infrastructures (50%) with plans to integrate automation (43%) to help automate security measures. To accomplish this, executives (75%) reported shifting more of the IT budget into security automation.

Respondents keep tabs on what's happening in the marketplace, and two-thirds reported that high-profile data breaches at peer companies were the most influential event that affected their own security planning.

Executives estimated the cost of an attack at 3.6 million USD/EUR/GBP/RMB, and more than one-third have paid after a ransom attack.

64%

have been attacked in the past 12 months

FINANCIAL/INSURANCE

Corporate networks are the lifeblood of finance companies' businesses, which is why this vertical is likely to invest more in security to protect its assets. For example, Deloitte[5], which suffered a cyberattack in 2017, said that it plans to spend 580 million USD on security over the next three years.

Finance companies are especially aware of what's happening at peer companies. Respondents (86%) reported that high-profile data breaches at peer companies were the most influential event affecting their own security planning.

Executives paint a picture of a forward march to network enhancements with plans to move to the cloud (68%), digital transformation plans (65%) and the integrating security automation (62%) ranking highest on planning and investment priorities.

This vertical is integrating and enforcing DevOps security by focusing on third-party testing (59%) and security tests built into the process (56%).

Executives estimated the cost of an attack at 2.3 million USD/EUR/GBP/RMB, and almost half have paid after a ransom attack.

59%

have been attacked in the past 12 months

[5] *Financial Times*, "Deloitte plans $600m of cyber security spending": https://on.ft.com/2K19aaR

Looking Forward

C-suite executives recognize the multiple pressures on their organizations to integrate new network technologies, transform their businesses and defend against cyberattacks, which are growing in frequency and complexity.

As more companies add a mix of multiple public and private cloud environments to their IT architecture, the introduction of new vulnerabilities puts corporate and customer data at risk.

Executives know that their networks are penetrable by hackers and are ready to embrace automated processes as part of their security protocols. Increasing infrastructure complexity, digital transformation plans and integration of artificial intelligence impact their thinking about security planning and budget allocation.

The stakes are high. Security threats can seriously impact a company's brand reputation, resulting in customer loss, reduced operational productivity and lawsuits. The results of this C-suite survey reinforced the priority that cybersecurity maintains in the minds of executives around the world.

ABOUT THE RESEARCH

On behalf of Radware, Merrill Research surveyed 232 executives in April 2018 — with nearly equal distribution of respondents from AMER, EMEA and APAC. To participate in the *2018 Executive Application & Network Security Report*, respondents were required to be a company with at least 250 million USD/EUR/GBP/RMB in revenue and hold a title of senior vice president level or higher. By design, the survey required at least half of the respondents to be C-level executives, though this year's research attracted far more C-level corporate leaders. About half of the companies in the survey have 1,000 to 9,999 employees, averaging about 3,700. AMER respondents skewed highest in average number of employees at nearly 4,300.

radware

www.radware.com

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.