C-SUITE PERSPECTIVES:

From Defense to Offense — Executives Turn Information Security Into a Competitive Advantage

2019 EXECUTIVE APPLICATION & NETWORK SECURITY REPORT

Table of Contents

Executive Summary

Annually, Radware publishes the findings and analysis of a survey of senior executives from AMER, EMEA and APAC to gain a better understanding of the perceptions of current cybersecurity challenges and opportunities for C-suite-level executives. The *2019 Executive Application & Network Security Report* reveals that securing networks and digital assets is more than a necessary operational cost managed by the IT department. Rather, cybersecurity is a critical business driver that requires boardroom attention.

At the core of every business decision is a calculation about managing risk. Executives in the C-suite must balance a wide range of variables in the pursuit of profitability. What products and services do customers want, at what price? What investments make sense to drive long-term growth? How can the organization get more efficiencies out of its supply chain?

The respondents of Radware's C-suite survey understand that as their digital environments continue to increase in complexity, their vulnerability to cyberattacks increases commensurately.

The topic of cybersecurity continues to receive executive-level attention. Boards are regularly reviewing the true costs of cybersecurity attacks, simulating crisis communications plans for black swan events and building security features and functionality into their new business platforms. The ultimate goal is to find ways to reduce their risk exposure by proactively aligning network security strategies with business objectives.

Organizations have shifted their management philosophy around information security, viewing it as an investment and weaving it into their respective business strategy. This creates a culture where there is a focus on securing networks and digital assets at every level so that organizations can leverage cybersecurity as a market advantage with customers and supply chain partners.

C-Suite Perspectives:

From Defense to Offense — Executives Turn Information Security Into a Competitive Advantage

Radware surveyed more than 260 senior executives worldwide to discover their perceptions about the importance of cybersecurity to their organizations. Results revealed that the severity of the threat landscape, the mounting cost of attacks and the potential long-term negative impact on business operations weighed heavily on the minds of high-ranking management. Safeguarding the customer experience is now a business driver that warrants consistent C-suite guidance.

IMPACT ON BUSINESS IS LONG LASTING

Executives ranked the top three impacts on their organizations:

1. Customer loss **(45%)**
2. Brand reputation lost **(44%)**
3. Revenue lost **(42%)**

COSTS ARE RISING EXPONENTIALLY

The costs associated with attacks are trending up at a far faster rate than overall attack growth.

AVERAGE COST OF AN ATTACK INCREASED
YoY from **3M to 4.6M** USD/EUR/GBP*

REPORTS OF ATTACKS COSTING
10M USD/EUR/GBP or more
doubled from 2018*

*Companies above $1B annual revenue

CUSTOMERS FEEL THE PAIN

Data breaches broke hard-earned trust with customers.

30% average churn after a breach

$100K average investment to win back customers

EXECS ARE FOCUSED IN THE BOARDROOM

C-Suite executives played an active role in cybersecurity strategy and management.

98% Cybersecurity is becoming a shared responsibility across all members of the C-suite with 98% claiming some management responsibility for it.

82% of CEOs claim to have high knowledge of the topic

84% of CIOs and CTOs

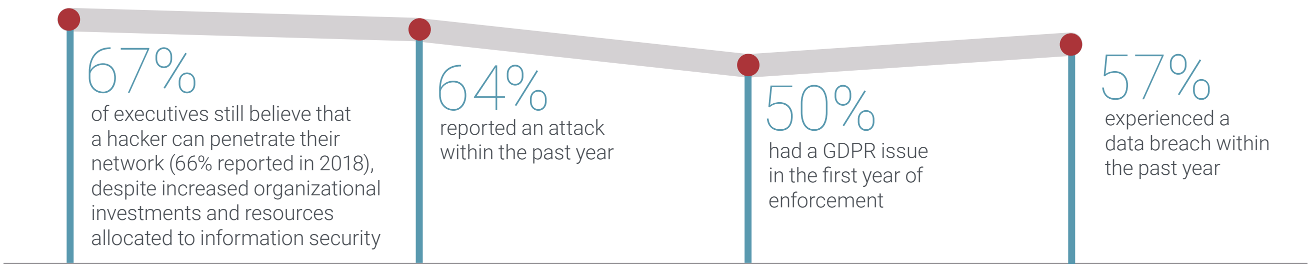
72% of other C-level titles and SVPs

72% of executives discuss cybersecurity at every boardroom meeting

1/2 of execs' time was spent on info security discussions

ATTACKERS ARE GAINING GROUND

As hackers refine their skills, attacks are more efficient and devastating.



67% of executives still believe that a hacker can penetrate their network (66% reported in 2018), despite increased organizational investments and resources allocated to information security

64% reported an attack within the past year

50% had a GDPR issue in the first year of enforcement

57% experienced a data breach within the past year

PUBLIC CLOUDS ARE NECESSARY BUT RISKY

Hosting data and apps in the cloud adds agility but also introduces risk.

73% Human error and malicious intent are contributing factors

Hackers broke through security of company **(31%)** or third-party provider **(37%)**

41% of employees neglected credentials in public forums

21% of insiders left a way in

DIGITAL TRANSFORMATION DRIVERS

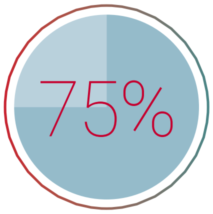
Senior execs continue to look to technology to advance business operations.

TOP-RANKED GOALS:

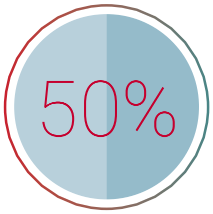
1. Improving information security
2. Business efficiency

SECURITY IS A KEY MARKETING FACTOR

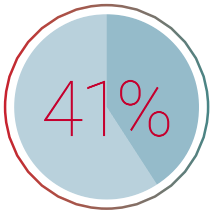
Organizations want customers to know about their security measures.



promoted the security of their products and services as a key marketing message



offered dedicated security products and services



had security features built into their products and services

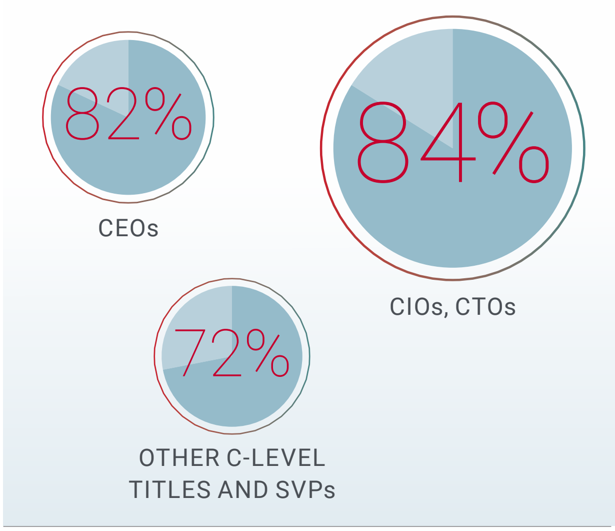
THE C-SUITE TAKES ON CYBERSECURITY

Hackers are getting smarter. As they figure out ways to make attacks more efficient, the level of devastation they cause intensifies. It only takes one network incident to cause loss of customers, brand reputation and revenue that can cripple an organization for years.

The impact on businesses can be disastrous. C-suite executives understand the risk, believe that they have a high level of knowledge about information security and increasingly view cybersecurity as a key business driver for which they must take responsibility.

As such, cybersecurity is finding its way onto the agenda of executive-level meetings. More than 70% of respondents said that cybersecurity is a discussion item at every board meeting. The executives estimated that about half of their time in the meetings was spent on information security discussions (42%–50%). Many organizations have digitally transformed to create faster, easier and more numerous access points for their customers.

RANKED THEMSELVES AS HAVING A HIGH LEVEL OF KNOWLEDGE ABOUT INFORMATION SECURITY



POSITIONING SECURITY AS A VALUE-ADD

Customers are very aware of the many data breaches that have happened in business-to-consumer and business-to-business industries in just the past few years. The impact of these successful cyberattacks has a far-reaching effect on all companies, not just the organizations that were breached. Confidence that interactions with any company are secure is damaged. A consumer confidence survey in the U.S. by **PWC** found that consumer trust is fading. Only 25% of the respondents said that most companies responsibly handle their sensitive personal data, while 15% thought that their data would be used to improve their lives. In the same survey, 87% of respondents said that they would not do business with a company that they don't trust to handle their data responsibly.

KEY FINDING:

Consistent across every region, 75% of executives reported that information security is a key part of their marketing messages, while 16% said that was a secondary message.

Dedicated security products and services were also offered to customers by 50% of responding companies. Forty-one percent offered add-on security features, and another 7% are considering building security services into their products.

In this "post-trust" era, organizations understand that customers are wary of sharing their personally identifiable information (PII). To build goodwill, companies can benefit from demonstrating to customers why they are trustworthy.

For example, in the spring of 2019, Apple launched an advertising campaign promoting the privacy protections on the iPhone, such as encryption of iMessage conversations and not keeping track of routes traveled in the maps app.

On a larger scale, many financial institutions, healthcare providers, software companies and other organizations market security and fraud services to enterprises and consumers. For example, **Chase** offers fraud protection services for business clients. Fidelity is launching a **new service** to add a layer of protection when users share account info with third-party applications and sites. PNC announced plans to launch an **account ownership authentication service** in 2019.

BUSINESS IMPACT:

Cyberattack Cited as a Factor for Outlook Downgrade

For the first time ever, Moody's, an American credit rating agency, cited cybersecurity issues as a factor when it slashed Equifax's rating outlook from stable to negative on May 22, 2019. Equifax suffered a massive breach of consumer data in 2017. In the first quarter of 2019, the credit monitoring company reported a $690 million charge related to estimated expenses to settle ongoing class action cases and potential federal and state regulatory fines related to the data breach.

Moody's announced in late 2018 that it planned to build cyber-risk calculations into its credit ratings, including associated costs, as the result of a data breach and reputational hazards.

TRANSFORMING INTO A MULTICLOUD ENVIRONMENT

While C-suite executives are taking on larger roles in proactively discussing cybersecurity issues, they are also evaluating how to leverage advances in technology to improve business agility. But as network architectures get more complex, there is added pressure to secure the new points of attack vulnerability.

Organizations continue to host applications and data in the public cloud, typically spread across multiple cloud providers, usually referred to as a multicloud approach. The multicloud approach enables enterprises to be nimbler with network operations, improve the customer experience and reduce costs.

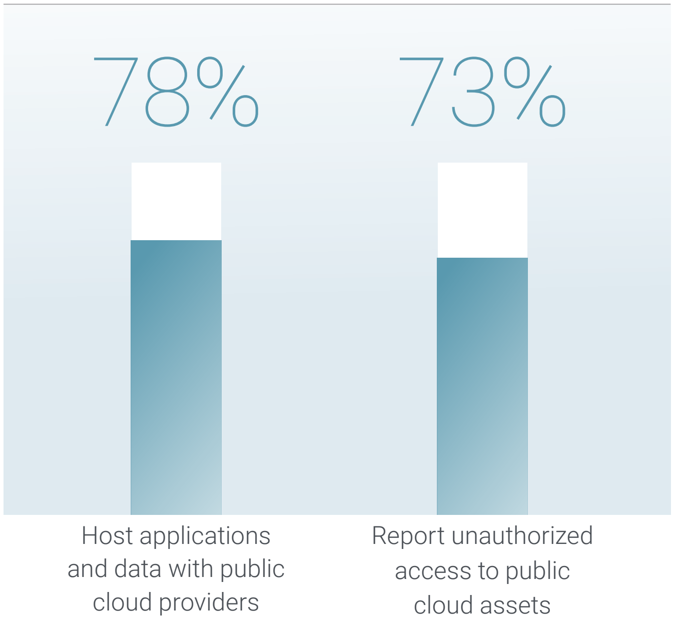
Every public cloud provider utilizes different hardware and software security policies, methods and mechanisms, which create a challenge for enterprises to maintain standard policies and configurations across all infrastructures. Plus public cloud providers generally only meet basic security standards for their platform only in an effort to standardize how they monitor and mitigate threats across their entire customer base. Application security of workloads on public clouds is not included in the public cloud offering.

Respondents reported that their companies are just as likely to use their own teams as they are to engage the cloud providers to secure their public cloud assets. Whichever choice is made, senior executives must lead the charge to develop and manage cloud security strategies that protect digital assets outside of their internal resources.

CONCERNS ABOUT THE PUBLIC CLOUD

Even with concerns about the security of public clouds, the trend continues for organizations to move applications and data to cloud service providers.

PERMISSIONS MANAGEMENT

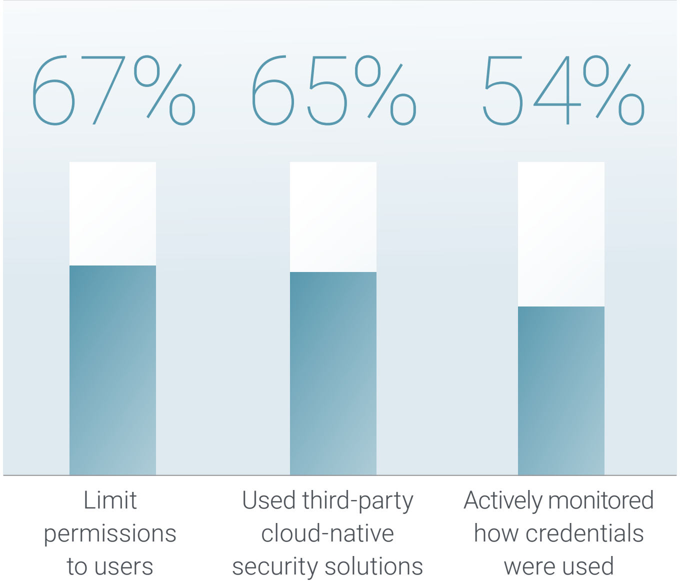


(Source: Radware 2018–2019 Global Application & Network Security Report)

KEY FINDING:

Almost three in five respondents expressed concern about vulnerabilities within their companies' public cloud networks.

WHAT MEASURES ARE ORGANIZATIONS TAKING TO SECURE PUBLIC CLOUD ENVIRONMENTS



The efficiencies of IaaS for network operations are somewhat offset by security concerns. Of the almost three-fourths who indicated that they have experienced unauthorized access to their public cloud assets, the most common reasons were that an employee neglected credentials in a development forum **(41%)** or that a hacker made it through the provider's security **(37%)** or the company's security **(31%)** or **(21%)** an insider left a way in.

Permissions for access to the public cloud were most often managed by limiting access or using third-party cloud-native security solutions. Two-thirds of the respondents used multiple techniques to manage permissions.

Permission management was consistent across regions, although executives from EMEA were the least likely to limit permissions (53%).

The Human Side of the Cloud

Sometimes the biggest threat to an organization's digital assets are the people who are hired to protect them. Whether on purpose or through carelessness, people can compromise the permissions designed to create a security barrier.

Malicious insiders are legitimate users who exploit their privileges to cause harm. Negligent insiders are also legitimate users such as Dev/DevOps engineers who make configuration mistakes or other employees with access who practice low security hygiene and leave ways for hackers to get in.

To limit the human factor, senior-level executives should make sure that continuous hardening checks are being applied to configurations to validate permissions and limit the possibility of attacks as much as possible. The goals are to avoid public exposure of data from the cloud and reduce overly permissive access to resources by making sure that communication between entities within a cloud, as well as access to assets and APIs, are only allowed for valid reasons.

VERTICAL FOCUS:

Executives from financial services were more likely to be "very concerned" about asset security in the public cloud and used third-party security solutions more than their counterparts from Retail and Telecommunications.

FOCUS ON DIGITAL TRANSFORMATION

Annually, the respondents are asked what their main goals are when integrating new technologies to transform their businesses. Improving information security has been the top-ranking response for the past three years. After dropping in 2018, this reason rebounded as the number one choice for more than half of the respondents in 2019. Business efficiency ranked number two. These two goals were top-ranked across all regions although "business efficiency" was more important in EMEA (50%) than in AMER (36%) and APAC (29%).

TOP GOALS FOR INTEGRATING NEW TECHNOLOGIES TO TRANSFORM BUSINESS

RANKING		2017	2018	2019
1	IMPROVING INFORMATION SECURITY	47%	38%	54%
2	BUSINESS EFFICIENCY	42%	37%	38%

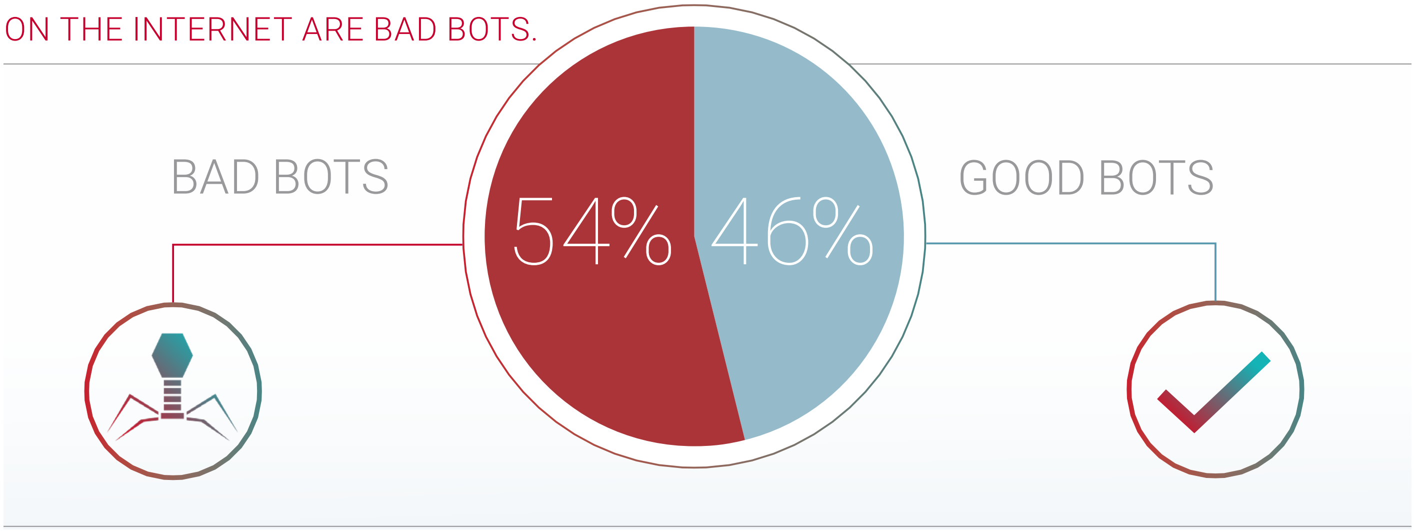
THE CONTINUED DRIVE FOR AUTOMATION

The trend continues to shift more budget into machine learning/artificial intelligence (AI) over the last two years.

This year, **82%** of the respondents reported an increase representing a continued focus on automation compared to **71%** who indicated the same response in 2018. **Eighteen percent** said that their budgets have not changed in this time frame.

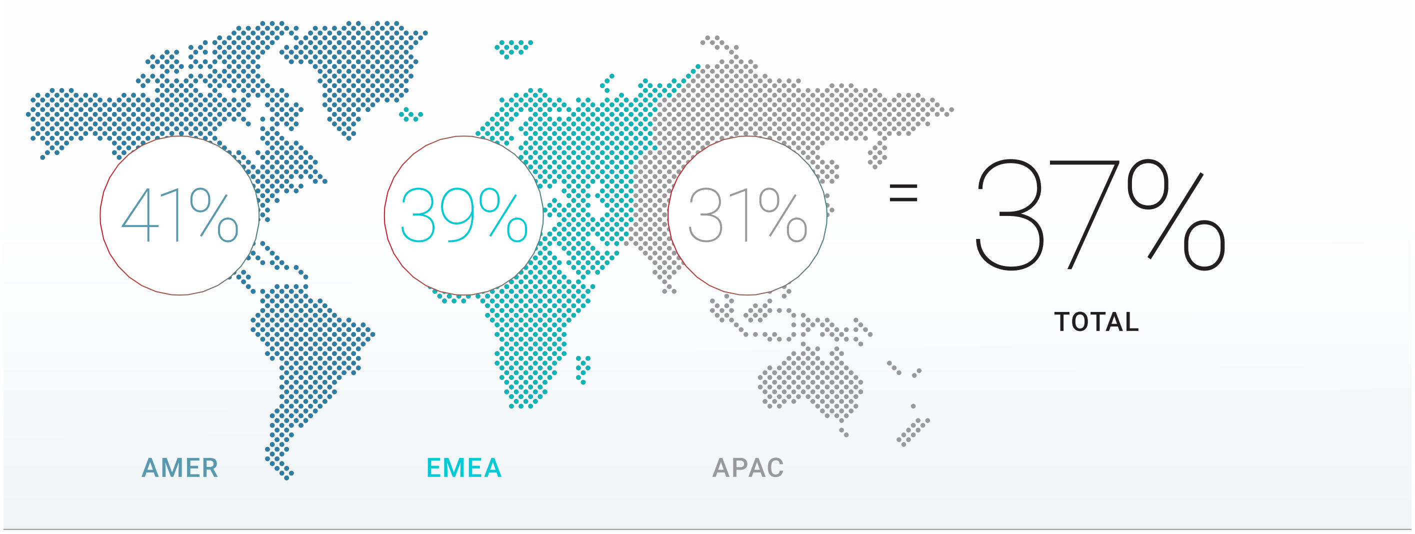
The need for increased automation in cybersecurity solutions is underscored by the increasing threat posed by next-generation malicious bots that mimic human behavior (see figure below). The time has arrived to fight automation with automation.

OVER HALF OF THE TOTAL BOT TRAFFIC ON THE INTERNET ARE BAD BOTS.



REGIONAL DIFFERENCES

% of Security Budget Allocated for Automated Security Systems (mean)



EYES WIDE OPEN TO THE SEVERITY OF THREATS

C-suite executives have a good sense of the relentlessness nature of attacks on their networks and applications — and the cost of a breach to their organizations, both in terms of finances and damage to customer relationships. The respondents are knowledgeable about how often they were attacked and what types of threats were most detrimental.

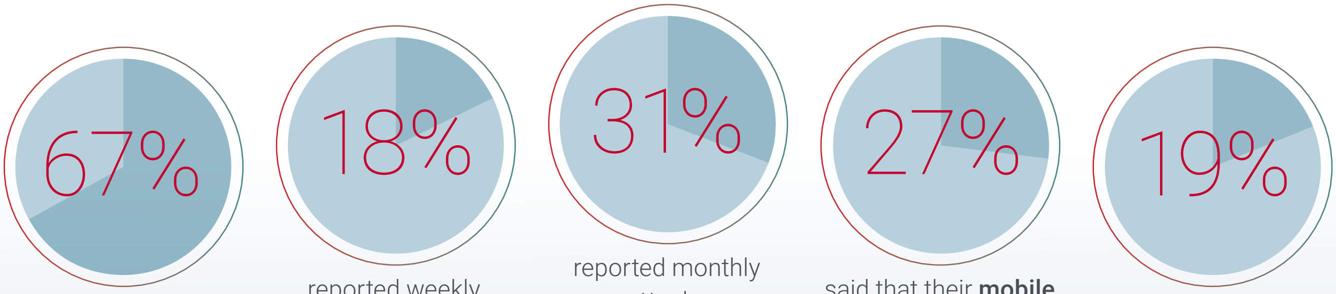
KEY FINDING:

The top three business impacts from a security threat were:

1. Customer loss	45%
2. Brand reputation loss	44%
3. Revenue loss and Productivity/ operational loss (tied)	32%

Legal action ranked third-highest as a concern in EMEA but ranked much lower in other regions.

C-SUITE VIEW OF CURRENT NETWORK THREATS



67% said that a hacker can penetrate their network — no change from 2018

18% reported weekly attacks on their network

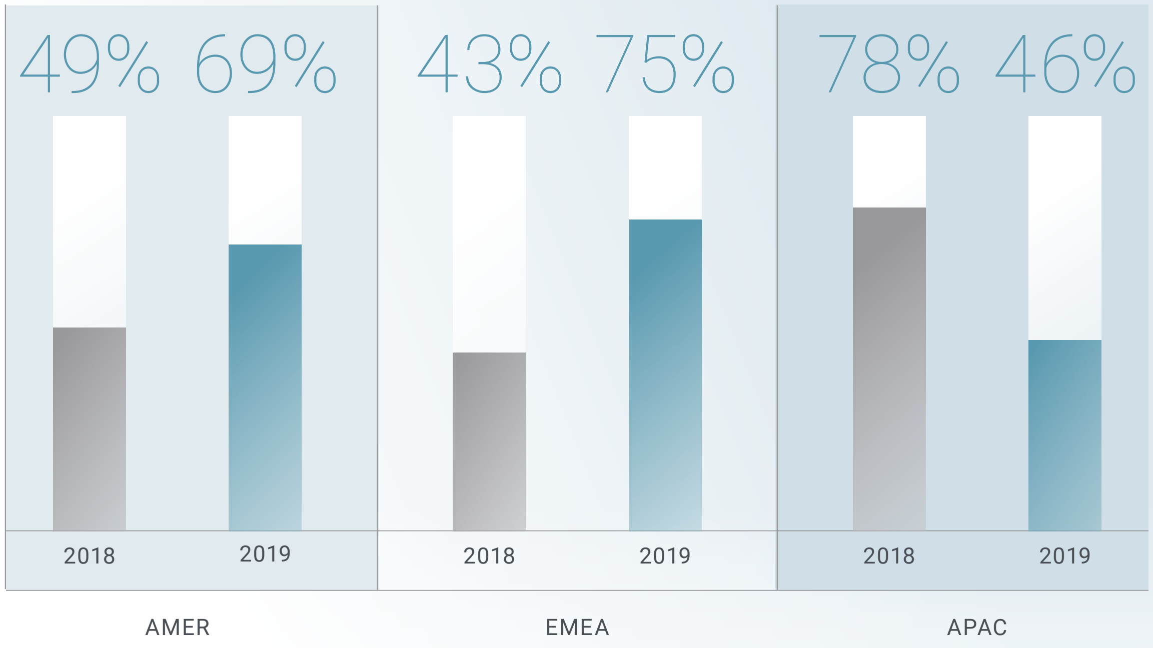
31% reported monthly attacks

27% said that their **mobile** apps were attacked on a daily or more frequent basis

19% reported daily attacks

REGIONAL DIFFERENCES

In the last 12 months, AMER and EMEA reported higher instances of attacks than during the same time period the year before, while APAC dropped significantly. APAC averaged the lowest number of attacks (four), while AMER reported 67 and EMEA had 93. Nearly 30% of the respondents from EMEA said that they had been attacked 11 or more times in the past 12 months.



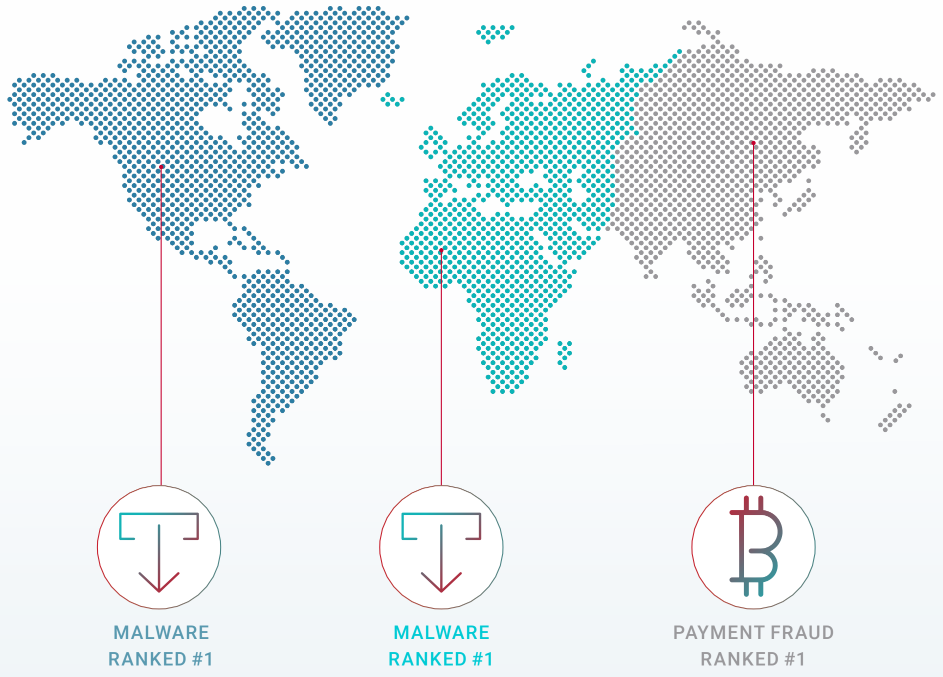
KEY FINDING:

With proper cybersecurity in place, it is likely that thousands of cyberattacks are mitigated daily in most corporate networks, and C-suite executives do not need to be made aware of them. In the past year, 64% of the respondents reported experiencing an attack that was substantial enough to warrant C-suite attention.

Executives understand the detrimental impact that cyberattacks can have on their organizations. About half of the respondents indicated that every type of cyberattack on the survey's list would be extremely detrimental.

REGIONAL DIFFERENCES

When ranking the level of negative impact that cyberattacks would have on their organizations, payment fraud (58%) and socially engineered threats (57%) ranked highest across all of the respondents. Executives from each region ranked the various attack types differently.



AMER
1. Malware
2. Payment fraud
3. Ransomware

EMEA
1. Malware
2. Socially engineered threats
3. Payment fraud

APAC
1. Payment fraud
2. Intrusions/advanced persistent threat
3. Socially engineered threats

Other attack types evaluated were web application attacks, denial of service and content scraping

CALCULATING THE COST OF A BREACH

Data breaches are expensive, and the costs are only going up. Those reporting attacks that cost 10 million USD/EUR/GBP or more almost doubled from last year — from 7% in 2018 to 13% in 2019. Half of the respondents estimated that an attack cost somewhere between 500,001 and 9.9 million USD/EUR/GBP.

KEY FINDING:

The average cost of an attack increased $1.6 million USD/EUR/GBP from last year.

3.0
MILLION
USD/EUR/GBP

2018*

4.6
MILLION
USD/EUR/GBP

2019*

*Companies above $1B annual revenue

ONE YEAR OF THE GDPR

The General Data Protection Regulation (GDPR) has been active in the European Union since May 2018. More than half of the respondents from EMEA experienced a self-reported incident under the GDPR in the past 12 months.

Every EU state has a data protection authority (DPA) that is authorized to impose administrative fines for improper handling of data. Fines can go up to 4% of a company's worldwide revenues for more serious violations. Article 83 of the GDPR requires that fines be "effective, proportionate and dissuasive."

The largest fine to date was levied against Google by France for €50 million for lack of consent on advertisements. In Germany, the social network Knuddels was fined €20,000 for insufficiently securing user data enabling hackers to steal user passwords. On the lower end, a sports betting café in Austria was fined €5,000 for unlawful video surveillance.

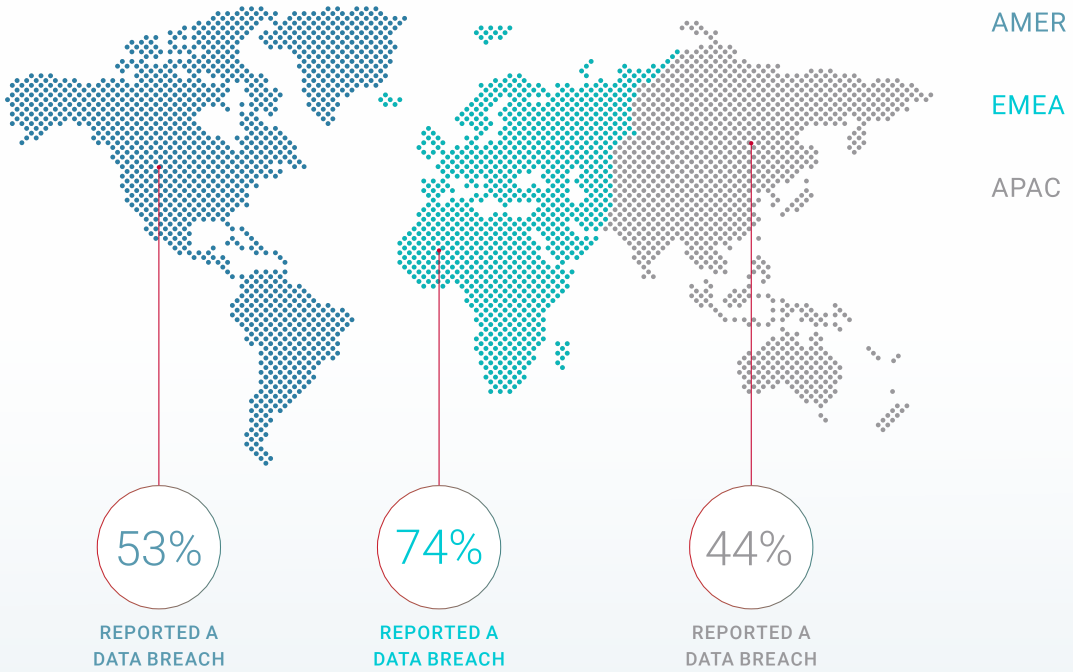
Almost 150,000 complaints about data handling have been received by DPAs so far. Most are about video surveillance and advertising calls or mailings, according to the EU Commission. Fines have not yet been imposed in many cases, but the potential for significant penalties is a potent motivation for compliance. C-suite executives in all regions should not let the leniency of the first year of GDPR enforcement lull them into complacency.

EXPOSURE RISK FROM DATA BREACHES

The threat of GDPR fines is just one risk facing organizations that experience a data breach. The danger is very real. More than half of the respondents said that they suffered a data breach in the past 12 months.

REGIONAL DIFFERENCES

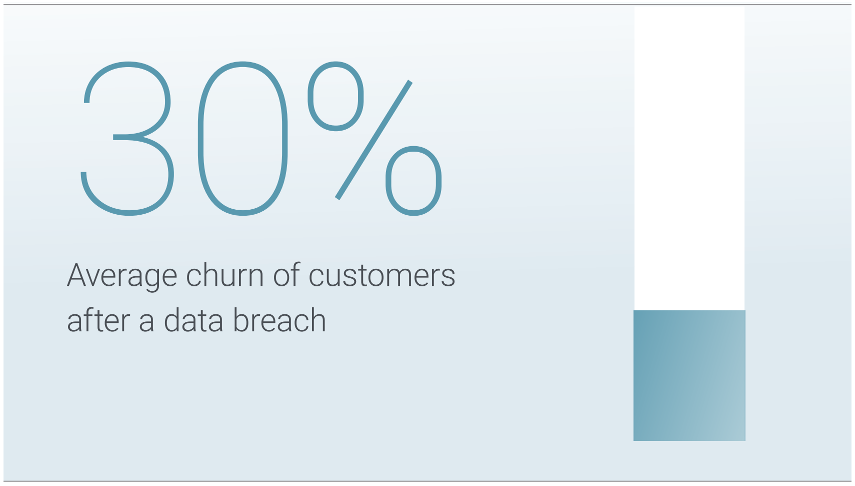
Reports of data breaches are the highest in Europe where half of the respondents also experienced a GDPR incident in the past year.



The repercussions of a data breach have a long-lasting effect beyond the initial recovery efforts and costs. Organizations spend billions to digitally transform their operations to support convenient ways for their customers to interact with them. Access to customer data enables companies to create more personalized experiences, but a data breach breaks the implicit trust needed to sustain that relationship. On average, the respondents reported that 30% of customers churn after a data breach. Customers in APAC were a bit more forgiving with a 20% churn rate.

After a data breach, churn was the highest (38%) at financial services companies.

CHURN

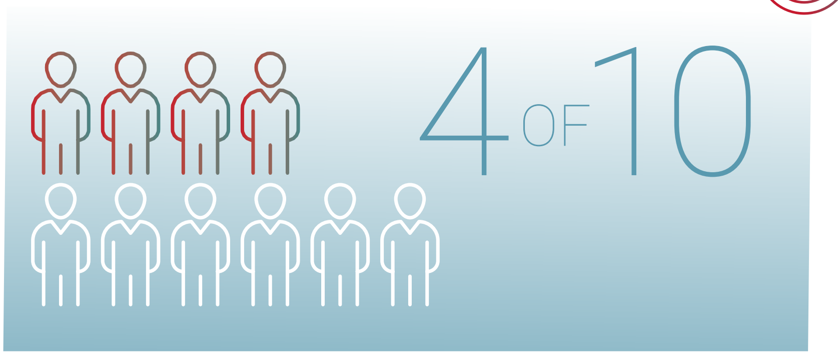


Customers are willing to fight back. Similar to last year, 37% of executives reported that customers have taken legal action against their companies after a data breach, with the highest rate of litigation (47%) in EMEA.

KEY FINDING:

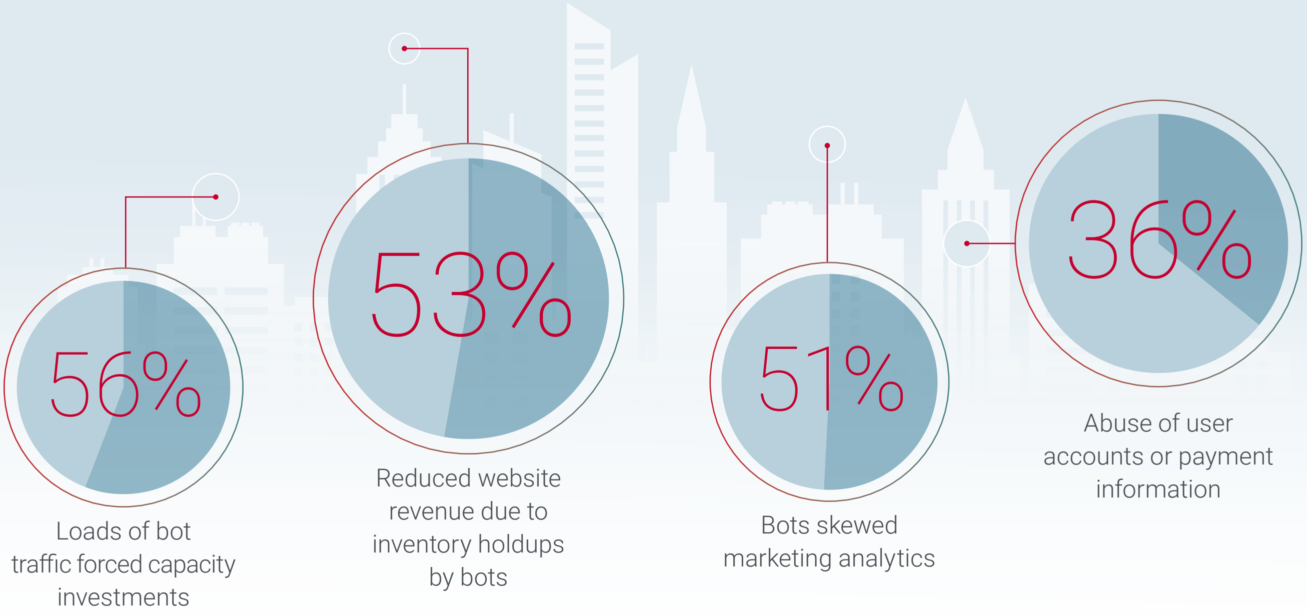
Executives estimated that, on average, it took an investment of 100K USD/EUR/GBP to win back customers after a data breach.

Executives were the victims of cyberattacks as well. About four in 10 reported that their personal information was exposed as the result of a data breach, similar to results from 2018. Exposure was the highest (47%) in EMEA.



IMPACT OF BOTS ON BUSINESS OPERATIONS

Of the respondents that claim to be able to detect non-human communications on their web properties:



WEBSITES AND MOBILE APPS ARE VULNERABLE

KEY FINDING:

Almost half of all executives believed that their websites were extremely or likely prone to attacks. More than one-quarter of the respondents reported that their mobile applications were attacked on a daily or more frequent basis.

Websites and mobile apps are the digital tools that customers use to interact with companies. About half of the respondents indicated that the impact of attacks on their company's website was stolen accounts, unauthorized access or content scraping. Two in five said that the attacks were launched by both humans and bots, while one-third credited humans only for the attacks.

Executives in AMER were more likely than those in other regions to say that their sites were extremely prone to attacks.

BOTS IN THE BOARDROOM

Bots are automated programs that run independently on networks to perform a series of specific tasks; for example, collecting data. Good bots are useful tools that automate processes and handle complicated interactive situations. Bad bots use the same technology to serve as weapons of attack and are one of the fastest-growing and challenging threats in the security landscape.

Bots were a topic of discussion in the boardroom. Most said that they have discussed the impact of bots on business operations at the executive level.

KEY FINDING:

Half of the executives acknowledged that bot attacks were a risk but were confident that their staff was managing the threat. Despite this confidence, the market for bot management solutions is still small and emerging, and is expected to experience a compound annual growth rate of 36.7% from 2017 to 2022, according to Frost and Sullivan. Two in five said that they relied on bots to accelerate business processes and information sharing. An equal number of respondents complained about how bots influence the metrics of their business unit. AMER executives were more likely than those in APAC to say that bots are cost-effective.

VERTICAL FOCUS:

Rankings of how frequently items regarding bots were discussed at the executive level vary by vertical.

	FINANCIAL SERVICES	RETAIL/ HOSPITALITY	TELECOM/ CARRIERS
1	Loads of bot traffic forced capacity investments	Reduced website revenue due to inventory holdups by bots	Bots skewed marketing analytics
2	Bots skewed marketing analytics	Abuse of user accounts or payment info	Loads of bot traffic forced capacity investments
3	Reduced website revenue due to inventory holdups by bots	Loads of bot traffic forced capacity investments, and bots skewed marketing analytics (tied)	Reduced website revenue due to inventory holdups by bots

The Impact of Cyberattacks on Business Insurance

Organizations purchase insurance to mitigate risk from event losses that may occur while doing business, for example, if a manufacturing plant catches on fire or a problem is discovered with a product requiring a recall. The damage from cyberattacks results in measurable tangible and intangible costs for organizations that fall victim. Can companies rely on their insurance providers for help? Maybe.

Mondelez, producer of well-known food brands like Philadelphia cream cheese and Cadbury chocolate, is suing Zurich Insurance for breach of contract. In 2017, Mondelez was hit by the NotPetya cyberattack, which disabled the company's ability to access network files and applications. The insurance provider cited the war exclusion clause in its contract with Mondelez to deny related claims because the U.S. government assigned responsibility for the attack to Russia.

Merck is also in the fight. The pharmaceutical giant filed similar suits against more than 20 insurance providers after its claims in relation to the NotPetya attack were rejected.

The legal fights could take years to resolve and will set a precedent about the validity of the war exclusion for cyberattacks blamed on foreign governments. In the meantime, companies can expect to bear the costs of cyberattacks on their own.

CHANGING VIEWS ON CYBERSECURITY

What does the shift in how cybersecurity is viewed by senior executives within organizations mean? This year's survey of C-suite executives finds that respondents recognized that cybersecurity was not just in the domain of the IT department any more.

The protection of public and private cloud networks and digital assets is a business driver that needs to be researched and evaluated just like other crucial issues that affect the health of organizations.

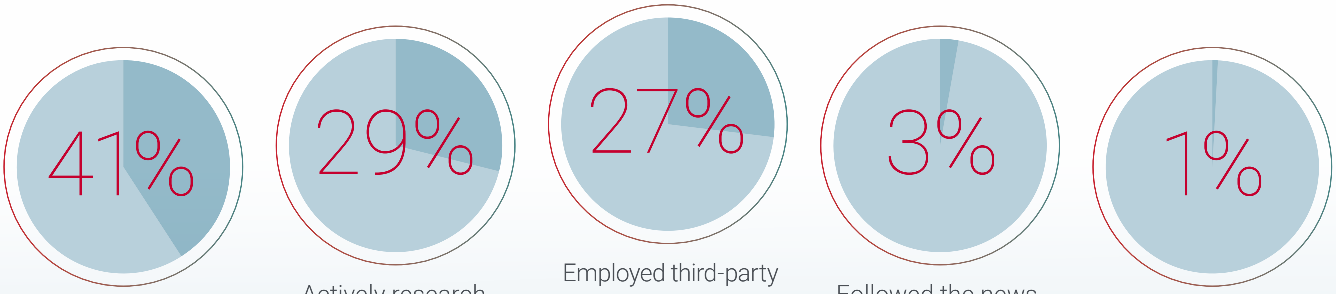
Just because the topic is being elevated to the boardroom doesn't necessarily mean that progress is being made. Executive preference for cybersecurity management skewed toward internal management (45%), especially in the AMER region (55%), slightly higher than in 2018. Yet the number of respondents who said that hackers can penetrate their networks remained static at 67% from last year's C-suite perspectives report.

As in the past two years' surveys, two in five executives reported relying on their security vendors to stay current and keep their security products up to date. Similar percentages also reported daily research or subscriptions to third-party research centers.

At the same time, the estimated cost of an attack jumped 53% from 3 million USD/EUR/GBP in 2018 to 4.6 million USD/EUR/GBP in 2019.

Executives have more knowledge about cybersecurity issues and reported discussing the impact of bots from a number of perspectives.

STAYING CURRENT ON ATTACK VECTORS



41%: Relied on security vendors to stay current and keep products up to date

29%: Actively research security threats on a daily basis in-house

27%: Employed third-party research center that provides active attackers intelligence information on a real-time basis

3%: Followed the news, but usually were already vulnerable at that point

1%: Said that it is an impossible task to stay current on all the latest cyberattack vectors

LOOKING FORWARD >>

The respondents ranked improvement of information security (54%) and business efficiency (38%) as the top two business transformation goals of integrating new technologies. In last year's survey, the same two goals earned the top two spots, but the emphasis on information security increased quite a bit this year from 38% in 2018 (business efficiency held steady from 37% in 2018).

Although the intent to enhance cybersecurity increases, actions do not necessarily follow. Often the work to deploy new technologies to streamline processes, lower operating costs, offer more customer touch points and be able to react with more agility to market changes proceeds faster than the implementation of security measures.

Every new touchpoint added to networks, both public and private, exponentially increases organizations' exposure and vulnerabilities to cyberattacks. If organizations are truly going to benefit from advances in technology, that will require the right level of budgetary investment.

The true costs of cyberattacks and data breaches are only known if they are successful. Senior executives who spend the time now to figure out what cybersecurity infrastructure makes sense for their organizations reduce the risk of incurring those costs. The investment can also be leveraged to build market advantage if organizations let their customers and suppliers know that cybersecurity is part of their culture of doing business. Prevention, not remediation, should be the focus.

Securing digital assets can no longer be delegated solely to the IT department. Rather, security planning needs to be infused into new product and service offerings, security, development plans and new business initiatives. The C-suite must lead the way.

radware

www.radware.com

ABOUT THE RESEARCH

On behalf of Radware, Merrill Research surveyed 263 executives — with nearly equal distribution of the respondents from AMER, EMEA and APAC — between April 23 and May 6, 2019. To participate in the *2019 Executive Application & Network Security Survey*, the respondents were required to be employed by a company with a worldwide scope with at least 250 million USD/EUR/GBP in revenue and hold a title of senior vice president level or higher. About 60% of the companies in the survey have 1,000 to 9,999 employees, averaging about 5,400 employees per organization.

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.