radware

C-SUITE PERSPECTIVES

Accelerated Cloud Migration but Lagging Security

2020

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 executives. The *2020 C-Suite Perspectives Report on IT Security* reveals that the COVID-19 pandemic was a major accelerant for organizations to quickly move forward with the migration of business infrastructure and applications to the cloud.

The combination of a remote workforce and on-demand consumption of goods and services forced organizations to adopt an infrastructure that supports the digital experience. Simply put, the urgency of such an unanticipated and unprecedented situation removed many obstacles that had previously stood in the way of digital transformation plans — but not without complications.

Prior to the COVID-19 pandemic, more than 65% of organizations said that they had aggressive growth plans. When the pandemic hit, progress toward those goals contracted, as workforce reductions, reduced operating capital and lower revenue impacted respondents' companies. However, agile businesses quickly adopted operational efficiencies, embraced a more productive remote workforce and shifted their product offerings in favor of a contactless economy.

Even though the pandemic forced quick decision-making, most respondents planned to make these changes permanent and position their organizations well for future challenges. In fact, more than half of the respondents expected to return to growth by the 2021–2022 time frame. However, such rapid digital transformation has created IT security gaps due to a lack of understanding of the threat landscape and the perceived security that public cloud vendors provide.

In the mad dash to the cloud, organizations are losing control and visibility of cybersecurity.

During their move to the cloud, organizations unintentionally created challenges by trying to fit their on-premise workloads into a new environment. They also relied on third-party hosting providers to secure their IT infrastructure. Both of these factors contributed toward the creation of gaps in their security posture.

Executive Summary (continued)

Radware surveyed more than **260 senior executives worldwide** to discover how the COVID-19 pandemic affected their digital transformation plans. Results revealed that the C-suite drove quick action to address immediate needs and position their organizations well for the future by hastening timelines for cloud migration. But now it is time to play catch-up with security to close the gaps inherent in cloud networks.

ACCELERATED MIGRATION TO THE CLOUD

76%

of the respondents said that the pandemic accelerated their plans for cloud migration.

SHIFT TO REMOTE OPERATIONS

MORE THAN

80%

expected that their companies will continue to support work-from-home employees at a higher rate than before the pandemic hit.

EMERGENCE OF NEW REVENUE MODELS

56%

of companies with interests in online ordering, home delivery, teleconference and streaming services saw an immediate uptick in revenue.

INCREASE IN ATTACK VOLUME

30%

reported an increase in cyberattacks after the onset of the COVID-19 pandemic.

EVOLVING NETWORK SECURITY NEEDS

35%

of cyberattacks required an incident response. Moving business infrastructure to the cloud increases the attack surface and number of access points that must be protected at a time when cybercriminals continue to find new ways to take advantage of the global pandemic.

Making Smart Decisions in Uncertain Times

How do you strategically plan your way out of a pandemic?

As organizations ushered in the new decade, executives were optimistic about business prospects; automation promised to propel operational efficiencies, and C-level management continued to invest in digital transformation strategies.

Then the COVID-19 pandemic hit, and the realities of the "new normal" took hold. Plans to transition business infrastructures to the cloud — initially slated for months or even years down the road — accelerated rapidly. Senior executives had to quickly meet the challenge of implementing strategies that didn't just address immediate needs but also positioned their organizations well for the long term.

Indeed, the pandemic was the catalyst for the C-suite to take decisive action. Organizations swiftly migrated business-critical assets and applications to the cloud, and as a result, many now feel well-positioned to return to growth. However, this digital transformation journey is far from over. Instead, executives must now shift their focus to filling network security gaps overlooked in the initial rush to cloud migration.

Think Fast, Act With Purpose

Senior executives made quick decisions that will have long-term implications. **Roughly 50% of the respondents** noted that the changes made regarding headcount, processes/applications, real estate assets and budgets are permanent.

Immediate Business Impact

In their 2019 business plans, more than 65% of the survey respondents indicated that they planned for increased growth in 2019. Thirty-five percent of the respondents noted a positive impact on headcount. It's possible that downsizing at some companies enabled them to fill strategic positions with qualified candidates who would not have been in the job market prior to the pandemic.

43%

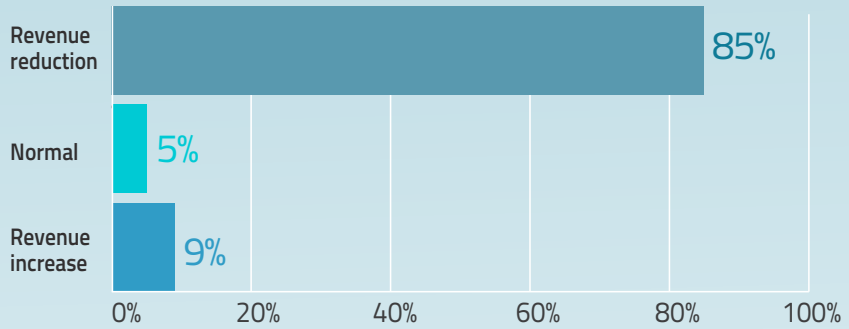
of the respondents reported **workforce reductions at their companies**.

34%

claimed benefits from **shifts in their business operations toward customization** (on-demand production).

Pandemic Revenue Jolts

Eighty-five percent of the respondents noted a revenue reduction as a result of the pandemic.



Mixed Aftershocks

There was an inverse relationship between operational efficiency and business contraction. The greatest positive impact was realized in processes/applications. The real estate assets segment experienced the greatest negative impact.

	+ IMPACT	- IMPACT
Processes/applications	46%	29%
Budgets	37%	44%
Headcount	34%	43%
Real estate assets	32%	62%

Focus on Efficiencies

C-suite executives quickly identified operational efficiencies to control costs and continue to support customers, suppliers and employees, including:

- Optimizing capex/opex
- Reducing the workforce
- Cutting back on real estate assets
- Shifting to a remote workforce
- Building robust digital infrastructures
- Transitioning IT infrastructure to the cloud
- Adopting artificial intelligence (AI), machine learning and automation technologies to reduce manual processes/errors
- Deploying differentiated security solutions

More than half of all respondents anticipated increased growth in 2021–2022 based on changes that they are implementing now.

40%

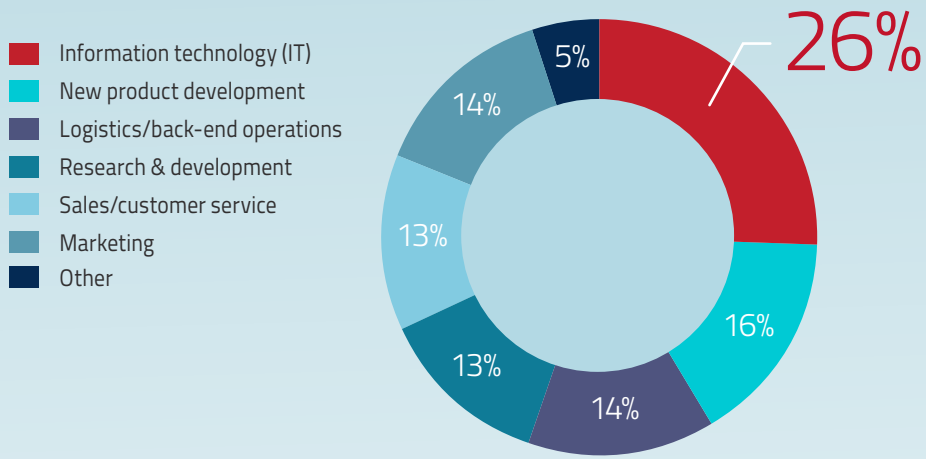
of the respondents said that their **organizations reduced headcount or eliminated positions** because of the COVID-19 pandemic.

20%

of the new funds allocated to IT budgets will be devoted to infrastructure enhancements, more than any other IT expenditure.

Redeployment of Investments

The response to the pandemic caused C-suite executives to shift financial resources. The respondents indicated that they plan to redeploy funds.



VERTICAL VIEW: Network Security Challenges

Accelerated decision-making has long-term implications for vertical markets.

Financial Services

More than **33%** planned to make their real estate changes permanent, while nearly **50%** expected to do the same with budgets.

Telco/Service Providers

33% planned to make assets/real estate changes permanent, and **39%** planned to make budgetary changes permanent.

Retail

39% anticipated real estate changes becoming permanent, while **34%** expected the same with budget changes.

Ensuring Business Resiliency

What has the pandemic taught us about future-proofing businesses?

The COVID-19 pandemic put disaster recovery plans to the test. It globally affected nearly every aspect of an organization in a concentrated amount of time. **Organizations that had strong disaster preparedness plans and an agile IT infrastructure in place fared better than those that did not.** To better position their companies against continuing disruptions, C-suite executives have sharpened their focus on strategies that build resiliency.

- Acceleration of plans to migrate network assets to the cloud
- Adoption of machine learning, AI and automation to improve resiliency and business efficiency.
- Transition to a largely remote workforce
- Reduction in the amount of real estate and other assets related to operating expenses
- Capture of market share by adapting to the demands of a contactless economy
- Staffing of hard-to-fill strategic positions from a wider and geographically diverse candidate pool

C-suite executives understand that leveraging new technologies can help their companies respond more agilely as market forces change. The hope is that the need for speed in transitioning to cloud-based networks will produce long-term benefits in faster time to market for revenue-generating services and applications, improved customer experiences and more robust support for critical business operations.

Planning for Disruptions

The swift impact on business operations caused by the pandemic drew the C-suite's attention to hidden vulnerabilities. Survey responses revealed that executives have moved quickly to build resiliencies into their organizations with an eye toward long-term results.

Key measures are focused on:

- Increasing market share
- Seeking new revenue streams
- Advancing network infrastructure to better support remote operations
- Improving the customer experience

Moving to the Cloud

Organizations look to cloud service providers for network infrastructures that enable more agile responses to customer needs and deliver high availability and network performance while reducing operational costs.

The respondents anticipated that only 16% of their organizations' infrastructure and applications will be hosted on-premise in 2021–2022.

76%

of the respondents said that **the pandemic accelerated their plans for cloud migration**.

Respondents said that more than **50% of digital assets will be hosted in public or private clouds by 2022**, while hosted or outsourced data centers will house the remaining **30% of digital assets**.

Top Reasons for Investing in IT/Technology

The respondents ranked the priority of the outcomes that they hope to achieve from the integration of new IT technologies.

1. Increased market share
2. Improved supplier management
3. Creation of new sources of revenue
4. Increased shareholder value
5. Reduced operational expenses

VERTICAL VIEW: Network Security Challenges

Building more resilient companies entails special considerations for vertical markets.

Financial Services

69% reported making their IT infrastructures more resilient via multi- or hybrid cloud adoption and 79% via automation.

Telco/Service Providers

74% reported making their IT infrastructures more resilient via multi- or hybrid cloud adoption and 76% via automation.

Retail

More than any other vertical surveyed, 83% of the retail/e-commerce respondents were making their IT infrastructures more resilient via multi- or hybrid cloud adoption and 80% via automation.

Maximizing Support for Remote Workers

How will the shift to remote work affect digital transformation?

As the pandemic spread across the globe, most companies mandated their employees to work from home. Suddenly, organizations needed network infrastructures that could support remote workers logging in to access critical company systems. C-suite executives directed their IT departments to quickly pivot resources to support the altered workforce.

Along the way, companies and employees discovered that working virtually has its benefits and may very well become the new standard of working life. Although some organizations are beginning to have employees return to the office (in a social distance-friendly manner), others such as Google, Twitter and Zillow recently announced that their employees may work remotely indefinitely.*

The shift to remote work also fundamentally alters the need for real estate assets while broadening the talent pool for qualified candidates who are no longer limited by their geographic locations.

*Source: www.businessinsider.com/companies-asking-employees-to-work-from-home-due-to-coronavirus-2020

Work From Anywhere

In an effort to slow the spread of the COVID-19 pandemic, many employees began working from home.

95%

of the respondents indicated that their physical locations were affected by lockdown orders to some degree.

By 2022,

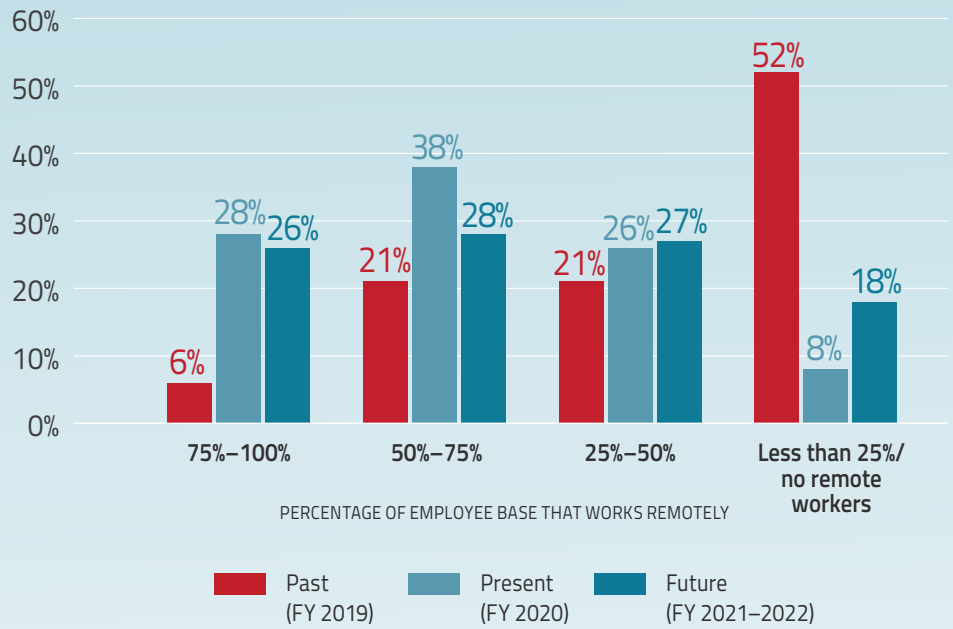
MORE THAN

50%

of employees will work remotely.

Remote Work Trend Will Continue

Respondents expected that their companies will continue to support work-from-home employees at a higher rate than before the pandemic hit.



Respondents stated that, in 2021–2022, they expect a **333% increase in business and expect more than 75% of their workforce to operate remotely.**

Conversely, the survey showed a **65% decrease in businesses that plan to keep most/all employees on-premise,** which represents a massive shift in business operations.

Networks Do the Heavy Lifting

The quick shift from the office to working from home spurred an unexpected business transformation as many organizations discovered that there are long-term benefits to the arrangement, including:

- Employee productivity significantly improved
- Employees reported a better sense of work-life balance
- Greater employee retention is likely because workers will enjoy more flexibility
- Companies now have greater access to candidates filling open positions that require in-demand skills

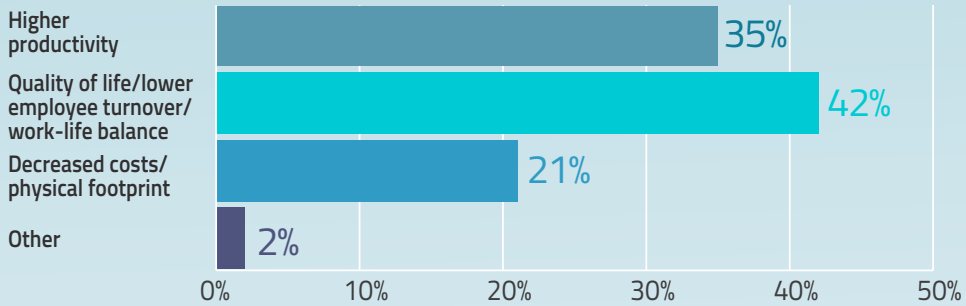
As organizations adopted a diverse employee pool, strategic and valued employees and candidates are no longer bound by geographical locations. Work-life balance has become a table-stakes requirement.

To support large-scale remote operations, organizations accelerated the adoption of managed services and the move to the cloud in their effort to build a resilient infrastructure.

Even though 43% of the respondents' companies had to reduce headcount, they reported a 46% increase in productivity by implementing remote work, improved processes, resilient infrastructure, automation and applications.

Benefits of Remote Work

C-suite executives moved quickly to enable remote workers. They now recognize some of the benefits of having more of their employees work from home.



VERTICAL VIEW: Network Security Challenges

Building more resilient companies entails special considerations for vertical markets.

Financial Services

The majority (58%) of the respondents expected **50% or more** of their workforce to remain remote during 2021–2022.

Telco/Service Providers

The majority (58%) of the respondents expected **50% or more** of their workforce to remain remote during 2021–2022.

Retail

The majority (54%) of the respondents expected **50% or more** of their workforce to remain remote during 2021–2022.

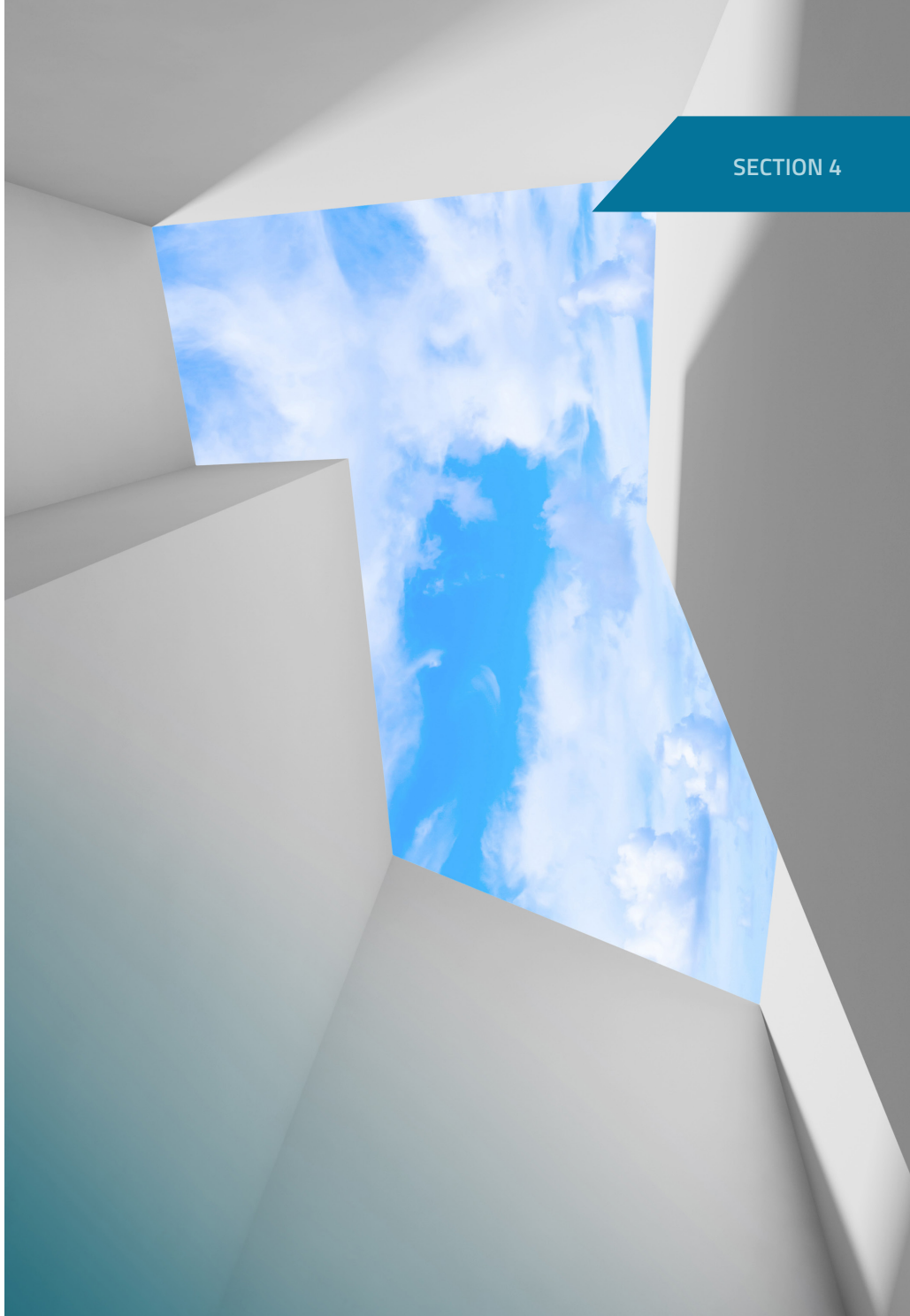
Managing the Evolving Security Threat Landscape

How has the pandemic affected network security?

The rapid shift in business operations significantly impacted the cyberthreat landscape. As companies fast-tracked the migration of digital assets to the cloud, they also inadvertently increased the attack surfaces from which hackers can try to gain access to their data and applications.

C-suite executives are moving quickly with network plans to support exploding customer and supplier demand for contactless interactions and the unplanned need to connect a remote workforce. Yet they are also aware that they are not fully prepared to adequately protect their organizations from unknown threats. The situation is further compounded by the cloud shared responsibility model, which says that cloud service providers are responsible for the security of the cloud while customers are responsible for securing the data they put into the cloud.

Cybersecurity is a key business driver that senior managers know must be incorporated into strategic planning at the highest levels. As the volume and sophistication of cyberattacks continue their relentless pace, organizations seek ways to automate detection and mitigation. Unresolved security incidents can be disastrous to companies already dealing with issues related to the pandemic.



Who Protects the Cloud?

Hosting applications and data in the public cloud is a proven way for enterprises to be nimbler with network operations, improve the customer experience and reduce costs. As more data moves to the cloud with the adoption of contactless payments and remote work initiatives, about **32% of the respondents** reported that they rely on public cloud hosting providers to secure their digital assets.

The issue with that approach is that every public cloud provider utilizes different hardware and software security policies, methods and mechanisms, creating 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 platforms because they want to standardize how they monitor and mitigate threats across their entire customer base. Lastly, the aforementioned cloud shared responsibility model further complicates things. Depending on the type of cloud deployment — software as a service (SaaS), infrastructure as a service (IaaS) or platform as a service (PaaS) — customer security responsibilities will be determined. The failure of customers to fully understand and adhere to the shared responsibility model is responsible for the majority of public cloud data breaches.

That leaves gaps in security, which hackers are more than happy to stay at home behind their keyboards to exploit.

Approximately

50%

of the respondents **were not confident** in their organizations' ability to effectively protect against unknown threats.

30%↑ reported an **increase in attacks** after the onset of the COVID-19 pandemic.

35% of cyberattacks experienced by the respondents **required an incident response**.

69% of the respondents spent more than 50% of their time on **network security-related discussions of issues**.

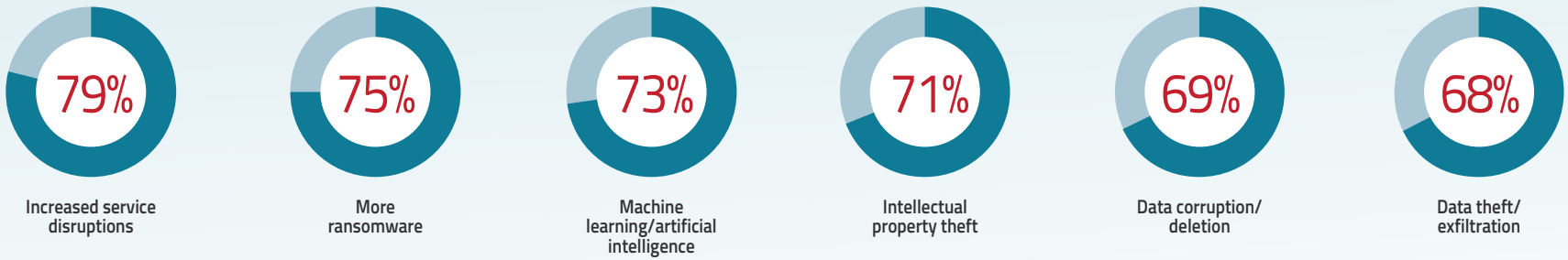
Current: Attack Vector Concerns

Organizations face a multitude of threats and attacks daily. Senior executives know that it is a struggle to scale their security infrastructures at the same pace as the technological advances they implement inside their networks, especially when timelines were accelerated by the pandemic.

The attack vectors that C-suite executives are most concerned about now are:

Future: Attack Vector Concerns

C-suite executives also have their eyes on evolving security threats. These are the attack vectors that they are concerned about as they develop over the next three years:



Understanding the Security Risks of Cloud Environments

What cloud security gaps do organizations need to address now?

C-suite executives should not expect the pace of decision-making to slow as the pandemic continues. Network migrations to the cloud, which likely would have taken place over five years, will be compressed into much shorter time spans. In the race to move digital assets to the cloud, most organizations did not have time to ensure basic network security compliance. More than 30% of the respondents said that they rely on their third-party providers to certify security management services.

Although the cloud enables organizations to respond rapidly to pandemic-related issues and market opportunities, the decentralized nature of this model adds complexity to how applications and computing resources are secured.

Organizations cannot simply move their critical business infrastructure and applications to the public cloud and assume that the hosting partner will take care of security. Cloud providers typically deliver the same standardized security across their customer base, essentially a "checkbox level" offering that meets basic requirements but does not meet the specialized needs of a specific enterprise. This depends on the nature of the application and the enterprise's readiness to move to the cloud as is or needing to be transformed into a cloud-native architecture. Organizations may assume that cloud providers are securing their digital assets without realizing how many gaps exist in the broadened attack surface.

To understand where the gaps exist in public cloud network security, organizations need visibility across all the different platforms from one holistic solution that enables management of the security posture by utilizing one common language. The goal is to be able to:

- Prevent attacks by reducing the size of the attack surface
- Detect and identify evolving threats
- Respond with accurate and effective mitigation

As network architectures get more complex, there is added pressure to secure the new points of attack vulnerability. Cloud environments introduce a significantly larger attack surface that requires protection from cyberattacks.

There is also a lack of visibility about which entity — the organization or the cloud service provider — is responsible for specific elements of network security.

In Radware's *2019 State of Web Application Security Research* report, 65% of the respondents said that they are not clear about security boundaries, and 53% of the respondents experienced data exposure as a result of misunderstandings with the public cloud provider regarding security responsibilities.

Increased agility and the pace of assets staged or de-staged make it challenging for organizations to realize and protect their rapidly changing security perimeter. C-suite executives should be mindful of potential security gaps as they continue to move digital assets to the cloud.

Indicators of Cloud Security Gaps

Senior executives are seeking ways to reduce risk exposures by proactively aligning network security strategies with business objectives. There are a number of questions they can consider to determine if their cloud environments have security gaps that need to be addressed.

Changes in network topologies and configuration

Challenges in adapting applications to cloud-native architectures

Changes in cloud workloads, such as containers, application programming interfaces (APIs), compute instances, storage, etc.

Sophistication of data access/authentication methods and shadow IT

Remote operations and workforce possibly resulting in noncompliance for key regulations such as HIPAA, GDPR and CCPA*

Management of distributed assets and environments

Management of third-party interfaces

Inconsistencies in third-party data access

Overall lack of consistent security posture and policy enforcement

*The Health Insurance Portability and Accountability Act, the General Data Protection Regulation and the California Consumer Privacy Act

Looking Forward

C-suite executives see the future as a globally dispersed, remote workforce catering to a customer base that primarily interacts with brands digitally, consuming goods and services from the comfort of home.

While the pandemic may have forced companies toward an acceleration into the cloud, C-suite executives embraced the opportunity to future-proof their organizations by building resiliency, honing budget management and adopting new processes and technologies. They quickly rethought their business, products and services and the infrastructure required to support their customers and employees in a contactless economy.

Throughout the next two years, organizations will continue to shift to the cloud and increase their investments in IT infrastructure and applications, in addition to machine learning, AI and automation. This will create more agility and efficiency in business operations and provide a better digital experience for consumers. These changes will require a powerful, complex security posture that is both agile enough to evolve at the speed of business and robust enough to ensure protection against a rapidly expanding threat landscape that specifically targets the cloud.

ABOUT THE RESEARCH

On behalf of Radware, Enterprise Management Associates Inc. surveyed 260 executives during July 2020 with nearly equal distribution of the respondents from AMER, EMEA and APAC. To participate in the 2020 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. Ninety-nine percent of the respondents indicated they have direct management responsibility for information security. About 80% of the companies in the survey have 1,000 to 9,999 employees. More than three-quarters of the respondents classified information technology as being very important to the operation of their organizations.

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.

© 2020 Radware Ltd. All rights reserved. Any Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: https://www.radware.com/LegalNotice/. All other trademarks and names are the property of their respective owners.