Balancing Cybersecurity Investments and Risks

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

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).
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:

- 47% Depend on IT security experts with long track records
- 32% Promote IT employees who show talent in security
- 9% Hire white hat hackers in-house
- 11% Use a combination of all three
- 1% Do not have an in-house security team

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.

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

- 33% prefer to manage security themselves
- 32% prefer their ISP/CSP or Carrier to provide security for them
- 19% prefer a combination of all three
- 16% prefer to depend on a security vendor

Talent Shortage Ahead

According to a recent Cybersecurity Ventures report, 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.

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

<table>
<thead>
<tr>
<th>No, and would not</th>
<th>Yes, we have in the past, but will not continue</th>
<th>No, but open to it</th>
<th>Yes, and will continue</th>
</tr>
</thead>
<tbody>
<tr>
<td>8%</td>
<td>21%</td>
<td>26%</td>
<td>45%</td>
</tr>
</tbody>
</table>

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.

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.

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

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.
DOWNLOAD C-SUITE PERSPECTIVES: TRENDS IN THE CYBERATTACK LANDSCAPE, SECURITY THREATS AND BUSINESS IMPACTS

LEARN MORE AT DDOSWARRIORS.COM
To learn more about today’s attack vector landscape, the business impact of cyberattacks or emerging attack types and tools, visit DDoSWarriors.com. Created by Radware’s Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cybersecurity.