



What Do Executives Think About Cybersecurity?

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 2019 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.

Here is a high-level breakdown of how C-suite executives feel about cybersecurity, its impact on business and its risk to the organization.

C-Suite Perspectives:

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

Radware surveyed more than 260 senior executives world-wide 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.

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

IMPACT ON BUSINESS IS LONG LASTING

Executives ranked the top three impacts on their organizations:



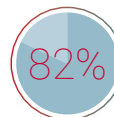
1. Customer loss **(45%)**
2. Brand reputation lost **(44%)**
3. Revenue lost **(42%)**

EXECS ARE FOCUSED IN THE BOARDROOM

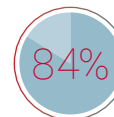
C-suite executives played an active role in cybersecurity strategy and management.

98%

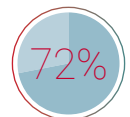
Cybersecurity is becoming a shared responsibility across all members of the C-suite with 98% claiming some management responsibility for it.



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%

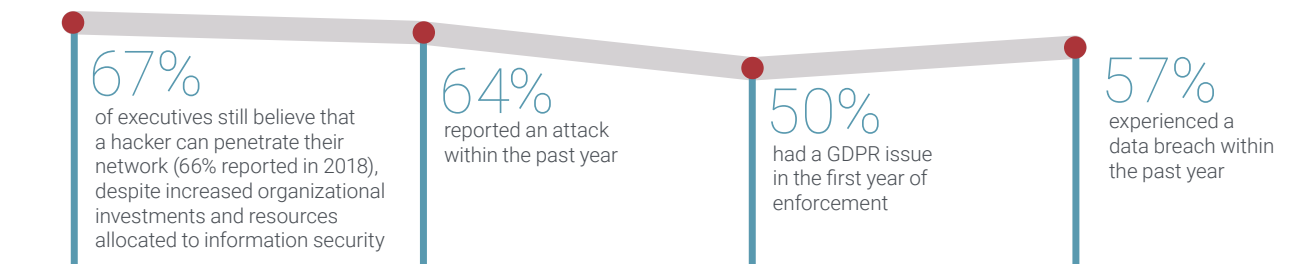
of executives discuss
cybersecurity at every
boardroom meeting

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.



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.

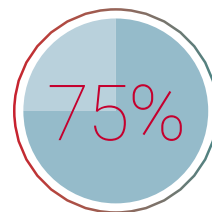


TOP-RANKED GOALS:

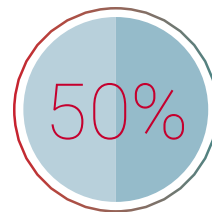
1. Improving information security
2. Business efficiency

SECURITY IS A KEY MARKETING FACTOR

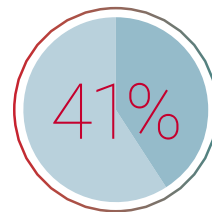
Organizations want customers to know about their security measures.



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

UNDERSTAND WHY SAFEGUARDING THE CUSTOMER EXPERIENCE IS NOW A BUSINESS DRIVER THAT WARRANTS C-SUITE GUIDANCE.