EXECUTIVE BRIEF

SECURITY CHALLENGES, THREATS AND OPPORTUNITIES – C-SUITE INSIGHTS

Insights for busy professionals
Read in less than 10 mins
Knowledge without the fluff

insight brief
RESEARCH. DISCOVERY. INSIGHTS.

radware

THIS EXECUTIVE BRIEF IS A SUMMARY OF THE REPORT:

Security and the C-Suite: Threats and Opportunities

CLICK TO ACCESS THE REPORT

INTRODUCTION

- The Executive Application and Network Security Survey surveyed 205 C-suite level IT executives in 2016 at companies with at least $50 million (or equivalent) in revenue, in the USA and the UK, to assess the biggest IT security challenges, threats, and opportunities they face.

DEFINITION

- Ransomware is a cyber-attack in which hackers use malware to encrypt an organization's critical data, making it unusable and then demand a ransom payment to decrypt it.
- The Internet of Things (IoT) is the umbrella term for the rapidly expanding array of networked devices, which includes utility smart meters, medical monitoring devices, and sensors used for everything from supporting public safety to automating manufacturing processes.

IMPORTANT DATA

- A growing number of C-suite IT executives, 82% in total, report that cyber-security is now a CEO or board-level concern: up from 75% last year.
- The majority of C-suite IT executives who have not fallen victim to a ransom-based cyber-attack said they would not pay; 77% of US-based and 91% of UK-based respectively. But of those that have fallen victim, 64% of UK-based executives did pay up, as opposed to just 29% of those in the US.

KEY POINTS

- The Internet of Things (IoT) is viewed as being a significant security concern in the next three to five years. A third of US-based C-suite IT Executives rated it as an "extremely likely" target, and 30% of UK-based executives agreed.
- The Internet of Things (IoT) creates a two-part security dilemma for businesses:
  1. Most IoT devices lack effective security capabilities and could therefore contain many unknown vulnerabilities which organizations must mitigate.
  2. There is also a potential risk from IoT devices themselves being hijacked and used as vehicles for an attack.
- Most people are unaware of how the IoT works or how their devices could pose a threat. They cannot be relied upon to maintain security capabilities and so the onus on securing devices will fall to security operations teams.
- According to C-suite IT executives the real impact of cyber-attacks was felt in damage to brand reputation, operational loss, and revenue loss. They also cited productivity loss, impact on share price value, unexpected budget increases, training / education and hiring requirements, and contract loss.

KEY POINTS (Cont.)

- The costs of paying to resolve a ransom-based threat differ significantly in the US and the UK. C-suite IT executives report an average US ransom of $7,560, while those in the UK pay an average of £22,217. These figures exclude ongoing situations.
- Automated security models involve enabling technology to initiate protection. Feeding data into a Security Information and Event Management (SIEM) system is not automated because it requires a human to make a decision.
- Automated security models are taking on a growing number of cyber-security tasks, largely because they are can work around the clock and rarely make mistakes. But the system will never be fully-automated and human talent remains crucial to an effective cyber-security structure.

IMPORTANT FINDINGS

- The financial impact of a cyber-attack is growing. More than a third of US executives reported a cost of $1M+, and 5% said an attack costs their business $10M+. In the UK, the cost per attack is generally lower, but 6% of respondents still reported it cost in excess of £7M.
- Cyber-security spending is on the rise, with around two-thirds of C-suite IT executives reporting increases of between 10% and 59% since 2015. But more than half of respondents did not know how much money or time their company committed to cyber-security.
- 83% of C-suite IT executives reported that their organisation has now invested in cyber insurance, with 42% of those investing within the last two years.
- While 36% of organizations have implemented security assessments for new technology within the past two years, C-suite IT Executives report that 41% of organisations still do not carry such assessments out.
- Hiring reformed hackers to test systems for vulnerabilities and combat attacks is becoming increasingly mainstream. They bring a unique insight and experience and 56% of organizations already employ them. As one respondent said "nothing beats a poacher turned gamekeeper".

CHALLENGES

- More than a third of C-suite IT executives surveyed said their organisation still had no business-wide cyber-security crisis team in place, comprising of representatives from HR, PR, and Customer Services.
- An organization's cyber-security standards are weakened if suppliers and partners don't also adhere to them. But 22% of C-suite IT Executives say these stakeholders are not addressed in their cyber-security processes, while a similar percentage also reported receiving no approaches from partners and customers about security enhancements.
- Paying to resolve ransom-based cyber-attacks can have unintended and undesirable consequences. On payment, hackers can choose not to unlock data and demand more money or may return to attack again later. Reports that you have paid could also reach other hackers, leading to additional threats from other attackers.

TAKEAWAYS

- Cyber-security responsibility should be clearly assigned by the board and C-suite of an organization to ensure transparency on current threats, protection strategy and where/how resources are being used.
- To counter cyber-security threats, around a third of C-suite IT executives in both the USA and the UK believe changes in technology, increased C-level awareness, and improved knowledge and education are all extremely important. Around 30% rate changes in process and policy as extremely important, while 20% highlight changes in resources.
- Organizations should have a pro-active plan to deal with ransom-based attacks in place, including
  - A security solution capable of protecting infrastructure from DDoS attacks.
  - An emergency response plan identifying responsible people and process, and where outside help is needed.
  - Careful monitoring of security alerts and triggers to enable the identification of real threats.
- Screening traffic as it enters and leaves an organization's network is lacking from many companies cyber-security models. But it is increasingly important to tackle modern threats that all inbound and outbound traffic is inspected, especially if it is encrypted.
- Three-quarters of C-suite IT executives are now using automated security models to defend against increasingly sophisticated threats. Many have put this in place after suffering a cyber-attack.
- Rather than giving into the ransom demands of cyber-criminals, organizational resources are better deployed in effective network, endpoint, and application security.

Click or scan to access the full report

CLICK TO ACCESS THE REPORT

radware

Radware is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Our award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down.

insight brief
RESEARCH. DISCOVERY. INSIGHTS.

Our team produces short documents for busy professionals, summarising longer reports and research papers so that readers can swiftly become acquainted with a large body of knowledge and decide whether or not to read the full source document(s).

We vet and qualify reports for relevancy and value to its intended audience before creating an InsightBrief document. Our editorial team is independent from the originator of the report, ensuring that the insights exclude sales or vendor centric messaging, thereby creating real value for our time-poor readers.