6 Cyber Security Concerns of C-Suite Executives

The role of today's information security executive is, in many ways, an unenviable position. The pressure to protect sensitive data and systems from a rapidly advancing threat landscape is enough to frustrate any CIO/CISO. The challenges of this role make the input and perspective of these executives particularly interesting. Recognizing the weight of this audience's perspective, Radware conducted a survey of more than 200 C-level security executives from the U.S. and United Kingdom. The goal: to understand their greatest challenges, threats and opportunities when it comes to information security.

From being held hostage to turning to former enemies for assistance, here are six of the biggest cyber security concerns pressing security executives from Radware's *Security and the C-Suite: Threats and Opportunities Report*.

C-suite Awareness is Growing.

Given the prevalence of cyber-attacks, it is no surprise that 82% of respondents say that security is now a CEO or board-level concern. In Radware's 2014 executive research findings, that was true for just under three-quarters of respondents. Meanwhile, 95% of 2016 respondents indicated that security is a very or extremely important priority within their organizations—with 41% reporting that their organization recently implemented a monthly board review of security measures.

Spending is Up. So is Uncertainty.

Approximately two-thirds of executives reported 10% to 59% increases in cyber-security spending since 2015. Yet in both the U.S. and the U.K., more than half of executives did not know exactly how much money and time their company has spent on security. Three-quarters have implemented, or are implementing, an automated security model, and 72% have invested in cyber insurance. Yet they're still losing sleep over a host of uncertainties, including the risk of insider hacks, the growing sophistication of cyber thieves, and vulnerabilities associated with home-based workers (42% told us they've recently implemented stricter security policies related to telecommuting).

Pay Up—or Else.

Radware's *Security and the C-Suite: Threats and Opportunities Report* noted significant growth in ransom as motivation for attackers—which increased from 16% in 2014 to 25% in 2015. Even though C-suite executives are unlikely to have full visibility to every security threat, one in seven respondents in the Executive Report reported that they experienced a ransom attack in the past year. More than half (54%) admitted to paying a ransom. In the U.S., the average ransom paid was $7,520; in the U.K., it was significantly higher at £22,218.

"Nothing Beats a Poacher Turned Gamekeeper."

In the face of increasingly complex threats, a growing number of companies are open to employing ex-hackers. In fact, 23% of respondents have already invited hackers to test their company's systems—and another 36% said they would be willing to do so.

A former hacker can help not only in testing for vulnerabilities but also in responding to attacks. As one survey respondent stated, "Nothing beats a poacher turned gamekeeper."

IoT Security is Top of Mind.

Executives in both the U.S. and the U.K. cited network infrastructure and IoT devices as the two most likely targets for hackers. The report identifies two major risks: that IoT devices will fuel new network vulnerabilities and that devices could be "taken over" by bots in order to steal sensitive information, launch attacks or enable other nefarious activities.

Suppliers and Partners Could be a Weak Link.

Among respondents, 44% have been including suppliers and partners in security processes for more than two years. Another 33% have begun doing so within the past two years. However, more than one-fifth (22%) are still not addressing suppliers and partners in their processes at all. When asked what partners and customers are asking related to enhanced security, two-fifths of executives said "none" or gave no specific answer.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about 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 cyber security.