Cyber Security Recommendations from the C-Suite

Security executives have a lot on their plate. They're grappling with a new breed of cyber-attacks, financially-motivated cyber assailants, and a bevy of new, connected devices (both corporate and employee) that bring unintended security risks to their organization.

But it's not all doom and gloom. C-level executives are relying on new technologies and best practices to fight fire with fire. They're turning to former enemies for help, getting more bang for the buck, and relying on automation to safeguard their organization's most critical information assets.

To garner the best practices of security leaders, Radware conducted a survey of more than 200 C-level security executives from the U.S. and United Kingdom. The *Security and the C-Suite: Threats and Opportunities Report* unearthed a series of top recommendations that organizations should heed carefully.

Practice #1: Perform greater screening on inbound and outbound data.

In open-ended responses, one executive mentioned future plans to increase screening on the traffic entering and leaving the organization's network. Such screening represents a significant gap for many organizations—and it's becoming increasingly important to address it. Radware has witnessed an increase in SSL/encryption, making inbound attacks more challenging to detect. Meanwhile, outbound traffic, especially when it's encrypted, is often not inspected.

Recommendation: Ensure that network/perimeter protections can inspect encrypted traffic without scale issues. Implement outbound traffic inspection capabilities.

Practice #2: When it comes to security, know what you're spending and why.

The Executive Report revealed an interesting paradox. A majority of respondents (82%) indicated that cybersecurity is a CEO- or board-level issue. Yet in both the U.S. and the U.K., more than half of executives did not know how much money or time their company has spent on security—from fighting cyber-attacks to implementing safeguards against hackers. Cyber security is simply too important, and poses too much risk, for that lack of executive awareness.

Recommendation: An organization's board and C-suite should assign ownership to ensure transparency on current threats, protection strategy and where/how resources are being used.

Practice #3: When facing a ransom demand, tread carefully.

With ransom attacks on the rise, the report uncovered another paradox. Eighty-four percent said if they were approached by cyber thieves, they wouldn't pay the ransom. Yet among those who were actually attacked, 54% said they did pay. Giving in to cyber thieves can be risky, as paying ransom may not stop the attack and, in fact, might increase the odds of additional incidents.

Recommendation: Flip the economic equation—investing resources into network, endpoint and application security rather than "donating" money to criminals.

Practice #4: Consider using hackers to test your security.

The results indicate an increased willingness to use hackers, and with good reason. Hackers bring unique experience and insight as companies work to keep pace with changes to the threat landscape and with the latest tactics, techniques and procedures.

Recommendation: At a minimum, conduct penetration testing and explore opportunities to engage white hat hackers to make the testing more realistic—and effective.

Practice #5: Automate security.

As the threat landscape becomes increasingly automated, protections need to be too. Forty percent of respondents indicated that have had automation in place for two or more years. That finding contradicts input from the Security Industry Survey, in which respondents said their organization's security is 80% manual. What this suggests is that executives may underestimate the extent to which certain security protections are still manual. That may include manual signature development for new attacks, as well as policy generation and vulnerability scanning/patching on applications.

Recommendation: True automation comes from enabling technology to initiate protections—not feeding data into a Security Information & Event Management (SIEM) system so that a human can make a decision. Explore multi-vector coverage through coordination of security components.

Case in Point: Best Practices in Action

One Radware customer exemplifies information security innovation. It delivers reliable performance for the company's technology backbone, with a DDoS protection strategy that incorporates proactive instead of reactive technology and uses behavioral analysis to minimize impact on legitimate users.

This online retailer's security team also uses a forward-thinking approach for evaluating return on security investments. In most companies, ROI calculations have focused on how much revenue would be lost per hour of downtime, how long it would take to reestablish a site after an attack and the likelihood of an attack taking the site down. More sophisticated analysis might also include cost to the brand—particularly if a company relies on its online presence for revenue.

This Radware customer took a more innovative approach. The security team began to consider how their ability to block bad traffic at the perimeter would positively affect the entire downstream environment. By building strong controls at every level of the infrastructure, the security team provided tools for the company's infrastructure and operations teams to process only legitimate traffic.

This resulted in a new, often overlooked, formula to measure the financial impacts of DDoS attacks. For DDoS attacks that will not affect the availability of online services, are those malicious attacks worth processing through the entire infrastructure? Aside from downtime, what are the downsides of having this traffic at any time in the infrastructure? Because of the velocity, volume and frequency of DDoS attacks, many data centers are processing massive quantities of malicious data. Processing that "illegitimate" traffic alongside online customers' legitimate traffic has significant operational and financial impact.

Once the security team started to calculate the cost of bad traffic that was now blocked at the perimeter and removed from downstream processing, they could quantify the return—and easily justify—the company's investments in security.

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.