2016 Cyberthreat Defense Report

Executive Summary

US DataVault-CyberEdge Group Report

CyberEdge Group's third annual Cyberthreat Defense Report provides a penetrating look at how IT security professionals perceive cyberthreats and plan to defend against them. Based on a survey of 1000 IT security decision makers and practitioners conducted in November 2015, the report delivers insights IT security teams can use to compare their perceptions, priorities, and security postures to their peers.

Notable Findings

- **Dwindling optimism.** More than half (62%) of respondents expect their organization to be compromised by a successful cyberattack in 2016, up from 39% two years ago.
- **Endpoint devices the weakest link.** When rating their organization's ability to defend against cyberthreats across various IT domains, respondents gave mobile devices the lowest marks, with laptops and desktops also near the bottom.
- **Mobile threats on the rise.** Two-thirds (65%) of respondents indicated there had been an increase in threats targeting their organization's mobile devices over the past year.
- **Endpoint self-remediation a top investment choice.** Of nine endpoint security technologies, self-remediation for infected endpoints (35.9%) was a top choice cited by respondents for acquisition in the coming year, trailing only containerization (37.9%).
- **Employees not helping the cause.** Low security awareness among employees continues to be the greatest inhibitor to defending against cyberthreats, followed closely by too much data for IT security teams to analyze.

Inevitable Infections

The conclusion that no organization is immune from cyberattacks has never been clearer. When asked to estimate the number of times their organization's network was compromised by a successful cyberattack within the past year, just over three-quarters (75.6%) of respondents admitted to at least one such incident, while more than half (51.9%) fell into the unenviable

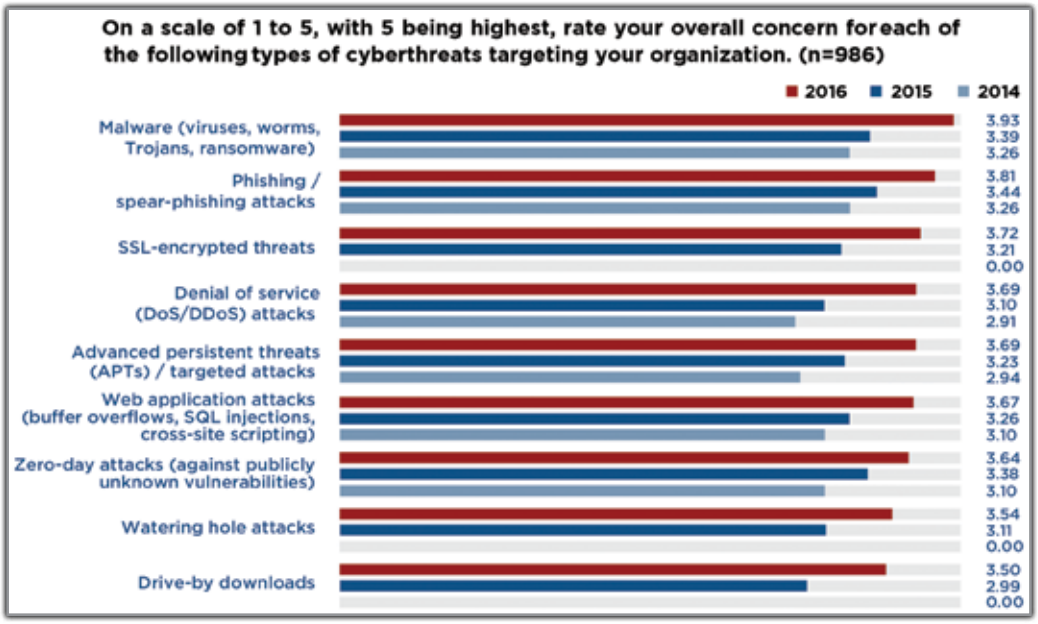

Figure 1: Relative concern by class/type of cyberthreat

Survey Demographics

- 1000 qualified IT security decision makers and practitioners
- All from organizations with more than 500 employees
- Representing 10 countries across North America, Europe, Asia Pacific, and Latin America
- Representing 19 industries

"Given the number of easy-to-use, feature-rich, and relatively affordable solutions available in the market, it is somewhat inexplicable to us that laptop backup practices are currently so lackluster – and we hope to see this change when we ask again next year!"

category of having been breached between one and five times. Expectations for the coming year are equally daunting, as only 11.6% consider it "not likely" that their organizations will be breached in 2016. As for types of cyberthreats causing the greatest concern for today's security practitioners, malware once again earned the "king of pain" title, followed closely by phishing/spear-phishing and SSL-encrypted threats (see Figure 1).

Under-protected Endpoints

The effectiveness of traditional endpoint security solutions, especially those that rely on signature-based detection technologies, has been in question for some time. However, with advanced malware now featuring countless tricks – such as polymorphism, active sandbox deception, and the ability to erase all traces of its presence after striking – the verdict is no longer in doubt. In fact, enterprise dissatisfaction couldn't be more clear, as a whopping 86% of respondents indicated their organization's intent to either replace (42%) or augment (44%) their current endpoint defenses. Factor in the ever-decreasing control IT has over end-user computing devices and the challenges of low security awareness among employees (and other users), and the case to consider solutions that preserve end-user data and speed recovery following the aforementioned "inevitable infections" becomes even stronger.

Deficient Backup Practices

One of the new areas of investigation for this year's study was to gain some insight into the extent that organizations are backing up the laptops of their mobile users to help guard against data loss stemming from cyberthreats. The answer: not so much (see Figure 2). On a global basis, only one in five respondents reported their organization regularly backs up more than 80% of mobile users' laptops, while more than a third back up less than 40% of these highly exposed devices.

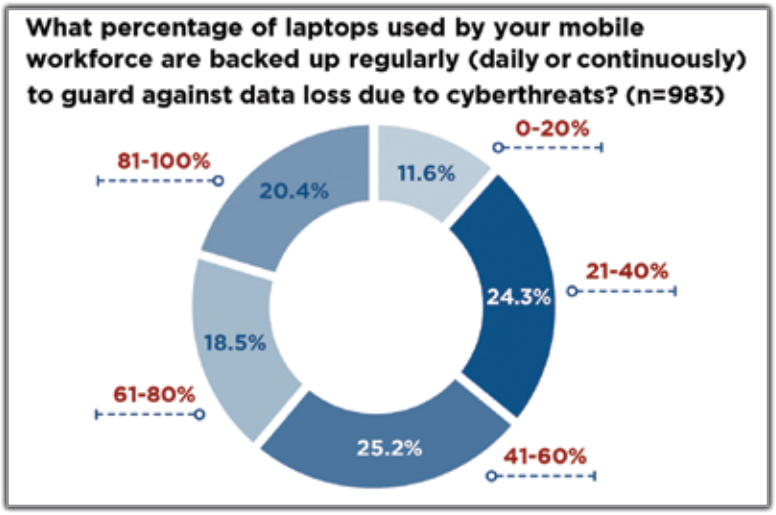

Figure 2: Percentage of mobile users' laptops backed up regularly

The Road Ahead

Security teams must ensure their organization's defenses keep pace with changes to both the IT infrastructure and the threats acting against it. The good news, at least for 74% of our survey respondents, is that their IT security budgets are expected to increase in 2016. When it comes to investing this windfall, some *additional* areas to consider include:

- User/entity behavior analytics and other user-centric security solutions;
- Advanced web application protection technologies capable of thwarting emerging automated threats; and
- Development of a formal cyberthreat hunting practice to better detect and isolate advanced threats.

About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our expert consultants give our clients the edge they need to increase revenue, defeat the competition, and shorten sales cycles. For information, connect to our website at www.cyber-edge.com.