CYBER DEFENSE MAGAZINE

eMAGAZINE

DECEMBER 2024

In This Edition

More Than Sales... How Brokers Can Play a Critical Role in Strengthening the USA's National Cybersecurity

Using Artificial Intelligence for Strengthening Email Security

Exploring Key Technology Trends for 2024

...and much more...

MORE INSIDE!

No Time for Cybersecurity Complacency in 2025

By James Edgar, CISO at Corpay

Cybersecurity is not a "set it and forget it" affair. It requires continuous vigilance, adaptability, and a proactive approach to stay ahead of increasingly savvy cyber criminals capable of attacks that can cripple a company in many ways. Even in the absence of any recent attacks, no company should fall into a false sense of security. Instead, it should reinforce the importance of maintaining and fortifying its defenses, because when it comes to cyberattacks, it is not a matter of “if” but “when.”

Every company must determine what information – including customer feedback, past attacks, performance data, and industry best practices – are most valuable for building, refining, evolving, and strengthening their cybersecurity program. A good place to start is understanding the current cybersecurity landscape, which can be done through a SWOT (strengths, weaknesses, opportunities, threats) analysis. To serve that purpose, each fall at Corpay, we conduct an annual survey of Chief Information Officers, Chief Information Security Officers, and other cybersecurity leaders and decision-makers from companies of all sizes. Before I dig into the 2024 survey findings, consider several recent high-profile breaches as a stark reminder of the persistent threat all companies face today.

Copyright © 2024, Cyber Defense Magazine. All rights reserved worldwide.

No Time for Complacency

CDK Global, a prominent ERP provider for car dealerships, suffered a significant cyberattack, incapacitating 15,000 dealerships' ability to sell, finance, or service cars. This incident underscores the vulnerability of critical service providers and the potential widespread impact of targeted cyberattacks.

Similarly, the Snowflake incident that led to a data breach at Neiman Marcus further highlights the evolving threat vectors targeting large enterprises. The LockBit ransomware group also made headlines with their attack on Evolve Bank, resulting in leaked data and heightened concerns about the security of financial institutions, including false claims of a Federal Reserve data breach that would have sent shockwaves through the financial markets. AT&T announced hackers obtained months' worth of data on its customers' calls and texts. They didn't get personal information, but it was an unnerving breach nonetheless.

Landscape SWOT

Even with these high-profile attacks as examples, only about one third of companies experienced a cyberattack in the past 12 months, according to the survey. The fact that such a high percentage of organizations avoided a cyberattack, or even better, prevented a cyberattack from happening, makes sense when you consider that about 70% of companies say they are comfortable with their current cybersecurity posture and capabilities.

However, nearly 80% of companies are still very or somewhat concerned about the risk of a cyberattack in the next 12 months, according to the survey. As a result, companies are putting their money where their mouth is, with 75 % planning to spend between 6% and 15% of their IT budgets on cybersecurity protection in the coming year. The problem is that 67% of respondents blame a lack of capital resources for why they aren't reaching their desired level of cyber protection.

It is probably no surprise to anyone reading that a fair portion of cybersecurity spending will be used on artificial intelligence (AI). In fact, more than 60% of companies are planning to evaluate and/or implement AI tools for cybersecurity purposes in the next 12 months, according to the survey. With each passing day, business cases are proving that the strategic use of AI can offset gaps in cyber defenses from a threat intelligence standpoint. AI can also fill huge staffing gaps caused by a lack of qualified cybersecurity talent (there are reportedly more than four million open security jobs and not enough people to fill them). The ability of AI tools to detect malicious software or a suspicious execution and quarantine it instantly so companies have time to determine next steps is an invaluable resource to off-set staffing shortages.

While AI is a wonderful use of budget, one place companies don't plan to spend cybersecurity dollars is paying off cyber criminals. While malware and phishing are by far the most common cyberattacks, bad actors might reconsider any plans for ransomware attacks because only about one in five companies would pay ransoms, according to the survey.

Copyright © 2024, Cyber Defense Magazine. All rights reserved worldwide.

Cybersecurity Recommendations for 2025

Given the current landscape, it is imperative for cybersecurity leaders to adopt a proactive stance. Here are five key recommendations for navigating 2025:

1. Establish a Clear Definition of Success: Success in cybersecurity should encompass both preventive and responsive measures. This means implementing robust defenses to thwart potential attacks and having a comprehensive recovery plan to minimize damage if an attack occurs.

2. Take Proactive Measures: Take advantage of the downturn in cyberattacks to develop and deploy proactive steps tailored to your organization's specific threats. This includes regular updates and patches, employee training on recognizing and responding to phishing attempts, and continuous monitoring for unusual activities. Check for any new networks or products that are exposed to the Internet and could be exploited.

3. Talent Acquisition: Hire and retain the necessary talent to execute your cybersecurity strategy effectively. This involves investing in skilled cybersecurity professionals who are adept at both defense mechanisms and incident response.

4. Leverage Advanced Technologies: Utilize advanced technologies such as AI and machine learning to enhance threat detection and response capabilities. These technologies can help identify patterns and anomalies that may indicate a potential attack.

5. Focus on Resilience: Ensure that your organization's cybersecurity strategy includes a strong emphasis on resilience. This means having robust backup systems, disaster recovery plans, and clear communication protocols to manage and mitigate the impact of a cyberattack.

Obviously, there isn't a one-size-fits-all approach, and every cybersecurity leader must establish and maintain a security program in collaboration with other internal stakeholders to best meet their specific needs now and in the future.

At the end of the day, creating a 100 % airtight defense isn't realistic. The goal is to stay ahead of these evolving threats, so a potential customer data breach or access to company IP becomes nothing more than a non-event recorded on a cybersecurity scorecard.

Conclusion

Whether a company has enjoyed the good fortune of declining cyberattacks in recent months or has been compromised repeatedly by malicious cyber criminals, a commitment to improving cybersecurity is critical for future success. The high-profile breaches underscore the need for continuous vigilance and preparedness, which seems to be embraced by many cybersecurity leaders heading into 2025. By defining success, taking proactive steps, and hiring the right talent, cybersecurity leaders can navigate the challenges ahead and bolster their defenses against the ever-evolving threats.

Copyright © 2024, Cyber Defense Magazine. All rights reserved worldwide.

About the Author

James Edgar is Chief Information Security Officer for Corpay (NYSE: CPAY), a global digital payments leader that helps automate, secure, digitize, and manage payment transactions on behalf of businesses across more than 100 countries in North America, Latin America, Europe, and Asia Pacific. I oversee the global Information Security and IT Compliance teams, which span four continents and multiple business lines. Before joining Corpay, I was the VP of Security Architecture, Risk and Assurance for U.S. Bank's payment processing division, Elavon. Prior to joining U.S. Bank, I led the Security Architecture and Risk team for Cox Communications, the third largest cable operator in the nation. I've served on the Steering Committee for the Payment Processors Information Sharing Council (PP-ISC), participated in the NIST Cybersecurity Framework (CSF) development workshops and has been actively involved in the governance, risk and compliance (GRC) community in Atlanta.

James can be reached online at https://www.linkedin.com/in/jamesedgar1/ and at our company website https://www.corpay.com/

Copyright © 2024, Cyber Defense Magazine. All rights reserved worldwide.