Safeguarding Success: FLEETCOR's Strategic Approach to Cybersecurity in 2024

January 22, 2024

Source: By James Edgar, Chief Information Security Officer, FLEETCOR

Is your company taking the necessary steps to protect from the ever-growing threat of cyberattack? I'm happy to share a few measures we are taking at FLEETCOR to protect ourselves and our 800,000+ business clients around the world.

Ransomware – The Triple Threat

Cyber criminals are becoming more brazen and creative in their use of ransomware, particularly a form known as "triple extortion." This is where the crooks steal and encrypt your data and then demand payment to 1) decrypt the information, 2) refrain from publicizing it, and 3) refrain from extorting your customers and suppliers. The implications are profound, as victims not only face financial losses but also damage to their reputation.

Facing this potential devastation, companies must prioritize their "cyber hygiene." At FLEETCOR, we have adopted a comprehensive strategy involving the deployment of defensive tools and continuous monitoring. We conduct executive "tabletops," simulating threat scenarios, and scripting responses according to our incident response plan. This proactive approach ensures that our plan is continuously updated and refined to outmaneuver potential threats.

Harnessing the Power of AI

In the quest for innovative solutions, AI emerges as a powerful ally in cybersecurity. AI can fill gaps in cyber defenses, offsetting the shortage of qualified cybersecurity talent. FLEETCOR recognizes the potential of AI to enhance threat intelligence and response capabilities.

Despite the industry's increasing reliance on AI, our survey of 350 businesses last year found fewer than 20% planned to deploy or test AI for cybersecurity in the next year. The more than 80% who don't plan to explore AI for cyber defense are overlooking an important tool at a critical juncture. Cybercriminals are using AI to invent new threats, so companies would be wise to use the technology to stave them off.

Adapting to New Regulations

Recent regulatory changes emphasize the increasing importance of cybersecurity for public companies. The U.S. now mandates that companies experiencing a "material" cybersecurity incident disclose the details within four business days. Additionally, regulations from the New York Department of Financial Services (NYDFS) and PCI 4.0 rules on data storage will impact IT leaders, necessitating a proactive approach to compliance.

At FLEETCOR, we regularly update our cybersecurity protocols to ensure adherence to new and existing regulations, and I would encourage every company to do the same.

Conclusion

In conclusion, the new year brings forth a challenging cybersecurity landscape, especially with the surge in ransomware attacks. FLEETCOR advocates for a proactive, strategic, and adaptable approach to cybersecurity, emphasizing proper cyber hygiene, leveraging AI, and staying abreast of regulatory changes. A vigilant cybersecurity stance is the cornerstone of a secure and prosperous 2024 for businesses worldwide.