STRENGTHENING CYBER RESILIENCE

Christopher Murphy, Managing Director, FTI Consulting, and Koroush Tajbakhsh, Director of Cybersecurity – ME, at FTI Consulting, on the power of proactive management.

As businesses of every size and industry capitalize on the benefits of rapid technological advances, cyber attackers are simultaneously refining their methods, launching increasingly sophisticatedattacksonostensiblysecurenetworks. Cyber threats manifest themselves in various forms, including data breaches, ransomware, and Distributed Denial-of-Service (DDoS) attacks, yet they all have the capacity to disrupt operations, inflict long-lasting reputational damage, and cause significant financial losses through business disruption and regulatory penalties.

The magnitude of cybercrime is staggering, with global costs projected to exceed $23 trillion by 2027, according to top cyber officials. In 2023 alone, the average cost of a successful cyber-attack has surged to $4.45 million. These statistics underscore the urgent need for a paradigm shift in how organizations approach cybersecurity.

BUILDING CYBER RESILIENCE THROUGH PARTNERSHIP

The modern business environment necessitates a cybersecurity strategy that adapts to an ever-evolving threat landscape. With the adoption of cloud computing, artificial intelligence, and the Internet of Things (IoT) into business operations, there is a critical need to transition from basic vigilance to a proactive model centered on building cyber resilience.

Organizations that are ill-prepared for cyber incidents often find themselves overwhelmed while grappling with containment, activating backups, coordinating with stakeholders, and navigating legal requirements. Given all of these moving parts, it is increasingly advantageous for organizations to partner with a single trusted provider, capable of managing the entire incident response process end-to-end. This approach aligns with the current trend of consolidating cybersecurity services and moving away from a fragmented provider landscape.

CHRISTOPHER MURPHY
Managing Director, FTI Consulting

Moreover, as the following evaluation of the three key stages of cyber incident response reveals, it is essential for organizations to have a trusted provider assess their entire cybersecurity environment and its risks before a threat becomes a reality, not afterwards.

PREPARING FOR THE UNEXPECTED

In a world of expanding regulatory compliance and enforcement surrounding cybersecurity, it is imperative for organizations to adopt robust protocols that ensure they do not become the lowest hanging fruit for malicious actors. These protocols help lay the foundation for continuous cybersecurity posture improvements by uncovering security gaps and providing mitigation strategies to address them.

Risk Assessment & Management involves identifying key assets, risks, and vulnerabilities in critical data, systems, and services. This includes mapping out legal and regulatory compliance requirements and reviewing third-party and supplier contracts to ensure cybersecurity and privacy provisions are included.

Incident Response Planning must be comprehensive, detailing protocols for internal and external stakeholder notification processes and requirements. This should be a collaborative effort involving all relevant parties within the organization.

KOROUSH TAJBAKHSH
Director of Cybersecurity – ME, FTI Consulting

Training & Collaboration is an essential component of preparedness. Regular training ensures staff are aware of potential attacks and understand their legal implications. Collaboration between employees and the company's IT and security teams is vital to maintaining alignment on cybersecurity policies. Building cyber resilience is a collective responsibility that requires ongoing engagement and education.

Moreover, organizations must evaluate their cyber insurance needs and assess whether current policy coverage is adequate for all potential cost scenarios. Similarly, cybersecurity due diligence is necessary for potential and current vendors and third parties to ensure robust security and privacy clauses are embedded into contracts.

RESPONDING EFFECTIVELY TO CYBER INCIDENTS

Effective incident response requires seamless coordination between IT, legal teams, and executive leadership to navigate both legal and operational challenges. The dynamic nature of cyber incidents necessitates a single trusted incident response provider that responds efficiently and orchestrates an expedited recovery.

Before activating the response plan, it is crucial to verify the plan's immediacy and to ensure legal and compliance aspects are managed by legal counsel. Clear engagement strategies are pivotal, and should include coherent internal messaging, strategic external notifications, and a plan for liaising with law enforcement if required. Response activities should align with privacy regulations, and notifications should be managed appropriately by legal counsel to ensure compliance with any regulatory requirements.

COLLABORATIVE REFLECTION AND LESSONS LEARNED

Post-incident reflection is crucial for recovery, legal compliance, risk mitigation, and managing potential repercussions. This phase must be led by executives and legal counsel, ensuring collective responsibility and organizational learning.

Legal compliance and evaluation efforts should focus on ensuring compliance requirements are met, documentation evidence is prepared for regulatory scrutiny, and a thorough debrief is conducted to update policies and procedures. External providers can assist in determining the incident's root cause, fortifying systems against future attacks, and updating training programs based on lessons learned. Ensuring data privacy through strengthened protection measures and updates to privacy policies is equally critical.

IN CLOSING

Taking a strategic approach to cyber resilience from the outset is fundamental to helping organizations rebuild a more secure and resilient environment. Proactive management serves as an effective countermeasure against cyber threats, positioning an organization for a more resilient future. ■