Preventing and/or responding to a cyber incident

Introduction or Enhancing Cybersecurity in a Connected World

Cyberattacks are a growing threat across all sectors, posing serious risks to the security of sensitive data, the continuity of essential operations, and the integrity of brand reputations. The financial implications can be staggering; for example, an IBM report highlighted that the average cost of a data breach in the healthcare industry alone reached $7.13 million in 2020. Moreover, the rise of remote work and the adoption of new technologies have heightened exposure to cyber vulnerabilities.

Recent incidents, such as those involving CrowdStrike, underscore the urgent need for organizations to enhance their cybersecurity measures and develop comprehensive redundancy plans. By doing so, businesses can better manage disruptions from cyber threats and protect crucial data and operations.

Ransomware Attack at Healthcare Payer

Many SEI associates were deeply involved in supporting a large healthcare payer when they fell victim to a ransomware attack which impacted the entire organization. Given the trusted relationship, additional SEI resources were tapped to help develop workarounds across the Marketing, Finance, Security and IT functions to mitigate impact and in parallel lead the recovery of services.

During the attack, SEI collaborated with the organization's vendors, functional areas, and IT teams to map the right approach and sequence of service recovery, from identification to testing and then restoration. Simultaneously, significant work was undertaken to stand up manual versions of typically online processes to ensure critical business needs could be continued throughout the outage. A group of SEIers worked to inventory all vendor relationships and then created reliable processes for restoring each connection based on how business was conducted.

SEI also coordinated the topics, inputs, and approvals of over 50 communications that the organization had to send to various stakeholders, such as members, providers, regulators, and media. SEI ensured that the communications were accurate, consistent, timely, and compliant with legal and regulatory requirements. A twice-daily call was held with key stakeholders to disseminate the latest information known at the time, capture workarounds, and actively troubleshoot next steps. These meetings continued until systems were fully recovered and workarounds were completed and/or closed.

After the attack, SEI conducted a lessons-learned session with parts of the organization and provided recommendations for improving their security posture, business processes, and disaster recovery plans. SEI also helped the organization implement the recommendations and monitor their outcomes. The payer was able to recover from the cyberattack, minimize the disruption to its operations and customers, and enhance its security and resilience for the future.

How SEI Can Help

To prevent or respond to a cyberattack, healthcare organizations need to adopt a comprehensive and proactive approach that covers both technical and business aspects of an attack. While some companies may already have a playbook to implement during an attack, many organizations only realize the importance after an attack has begun, when every day the operations are impacted has a direct effect on the bottom line.

Cybersecurity Prevention

IT & Security

- Understanding your current security posture is essential in order to protect your data and systems. SEI can help organizations comply with relevant regulations and standards, such as HIPAA, HITRUST, and NIST.

Cyberattack Response IT & Security

- Restoring online connections is a critical part of every cyberattack. SEI has the skills and expertise to aid organizations in the documentation, roadmap, and execution of a restoration process.

Project & Risk Management

- SEI can assist organizations interested in preventative scenario planning and disaster recovery exercises, using design thinking principles and techniques. This can help prepare for different types of cyber incidents, develop contingency plans, and test their readiness and resilience.

Operations

- Proactive organizations may be interested in establishing extensive documentation and quality control mechanisms for their mission-critical business processes.

Cyberattack Response

IT & Security

- During an attack, companies may need additional support integrating third-party vendors as well as monitoring security requirement status.

Project & Risk Management

- SEI has helped teams build out triage processes and prioritize key processes for recovery across large, complex departments.

Operations

- Manual processes will be established while the system is offline. Having a reliable quality control function is needed in order to minimize the impact of the transition.

Conclusion or Secure Your Future: Why Proactive Cyber Defense Matters

Adopting a proactive approach to preventing and responding to cyberattacks is a smart decision for any organization, regardless of industry. While developing a proactive response plan may seem easy to delay, it should be seen as a strategic investment. This intentional move can yield significant savings by mitigating potential damages from cyber incidents. Consider the invaluable resources you could save — not just in dollars but also in time, energy, and human capital.

As the digital landscape evolves rapidly, staying current with your organization's crisis management, data recovery, or security response strategies is crucial. Now is the perfect time to take action. We invite you to contact SEI to discover how we can enhance your cybersecurity posture. Our experienced team is ready to collaborate on improving your organization's readiness to identify, prevent, and respond to evolving cyber threats. Don't leave your security to chance — strengthen your organization's resilience today.