WARGAME
Summary Insights

Scenario Summary

- A massive amount of corporate data is exfiltrated and held for $50M ransom by ideological hackers
- Shortly after data ransom is known, employees report ransomeware affecting corporate mobile applications, forcing system shutdown decisions
- Law enforcement starts asking questions, raising legal and reputation risks from an investigation
- An emergency Board meeting leaves the CEO flustered; against CISO advice, she orders all IT systems backed up and client-facing portals locked down as a precautionary measure; also replaces current crisis management lead
- Public scrutiny grows and share price plummets as the Firm continues precautionary system shutdowns for days
- Customers and business clients allege negligence in data protection and threaten lawsuits to recover damages

"Lessons Learned"

- Breaches with enterprise-wide implications required integration and collaboration across the entire C-Suite, and may require difficult, high-risk decisions from across the enterprise
- CISO's typically were reluctant to relinquish control and believe they should run incident management, even when there are significant enterprise impacts - companies will default to the COO when the CISO is found to be ineffective
- CISO's who have experienced massive breaches recognize that high-risk decisions need input from across the enterprise
- Most incident management plans do not address the synchronization of technical and business decisions and implications
- Many companies excel at conducting technical exercises, but these exercises fall short when it comes to understanding the business/operational implications and clarifying the associated decisions rights of complex decisions
- Without a strong understanding of adversary intent and capabilities, remediation and recovery activities (such as bringing key systems back online) could be jeopardized
- Technical response teams need a buffer/intermediary between themselves and senior leadership (CEO, COO, Board, etc.)

Please feel free to contact us with questions or comments.

Nicole Monteforte
703.377.0823
monteforte_nicole@bah.com

Booz | Allen | Hamilton

WARGAME
Summary Insights

Summary Insights

1. ***Massive cyber breaches require an enterprise level response, led by a dedicated Crisis Management Executive.*** Far too often the CISO ends up serving as the overall incident manager; while the CISO is essential to managing the technical response, responding to massive incidents requires synchronizing business, legal, communications, as well as technical activities. Most companies would benefit from a pre-defined and dedicated Crisis Management Executive that has a broad enterprise view of the organization and capable of making critical decisions while understanding impacts to the entire business. A dedicated Crisis Management Executive will result in incident management teams that are effective and not paralyzed with determining decision authorities or establishing priorities for activities with enterprise-wide implications.
2. ***Cyber response plans and corresponding exercises must be holistic to include both technical and business considerations.*** While many companies have incident management plans, these plans often focus on the technical activities associated with responding to and recovering from an incident and lack a consideration of the business/operational implications of a technical action (i.e. does taking a specific system offline prevent a company from conducting core business activities?). Refining plans and conducting exercises that include not only technical response activities, but also include key business leaders will ensure that critical response and recovery decisions factor in business implications and do not result in unintended consequences.
3. ***A world-class cyber security program integrates solid business processes, IT tools and systems, and comprehensive cyber security plans.*** Failure to integrate, synchronize, and update systems and processes can lead to failures even after large investments are made in technology improvements. Malicious cyber activities will go undetected because monitoring tools are not integrated and not updated. Many companies make significant investments in monitoring, detection, and prevention capabilities only to leave those systems operating for several years without sufficiently updating them or adequately integrating them with new systems they bring on-line; thus creating significant gaps in their security.

Please feel free to contact us with questions or comments.

Nicole Monteforte
703.377.0823
monteforte_nicole@bah.com

Booz | Allen | Hamilton