BEYOND THE SECURITY TEAM: INCIDENT RESPONSE EMERGES AS ENTERPRISE PRIORITY

KEY ISSUE:

Enterprises need to better prepare their entire workforce to respond to cyber security incidents

The public nature of data breaches highlights cyber security incidents as more than a technical problem. Breaches cost the enterprise financially, in achievement of organizational goals and in brand reputation. This raises the stakes on incident response (IR) activities.

Significant security incidents require a full complement of activities to verify, investigate and remediate. These efforts range from digital forensics investigations to public relations exercises and even coordination with law enforcement or regulatory agencies. Many of these efforts require expertise beyond the scope of the traditional security organization.

Companies seeking to invest in incident response capabilities look to IT and security organizations to lead the way. However, traditional enterprise security programs often miss the mark by:

- Focusing narrowly on prevention.
- Considering incident response (IR) a subset of crisis management.
- Lacking standardization.

The growing number of data breaches in the news indicates a shift. For most organizations, breach is a matter of when, not if.

- The number of data breaches continues to rise in frequency and severity. Between 2004 and 2009, 900 total data breaches were made public and investigated by the United States Secret Service. In 2011, that number jumped to 761 in one year alone. Fast forward to 2015, the number of breaches increased by nearly 180 percent with 2,122 data breaches made public. [1]
- In 2014, the FBI issued an industry-wide warning to health care companies to strengthen their security practices as cyber threat was increasing. Within a year of that warning, Anthem reported 80 million records stolen. The breach included social security numbers and other personal details used for identity theft.[1]
- The U.S. Internal Revenue Service (IRS) reported the loss of approximately 100,000 taxpayer records. Initial estimates place the impact to taxpayers at $50 million in falsified claims. [3]

CHALLENGES AND OPPORTUNITIES:

Effective incident response begins with preparedness

Organizations respond to cyber security incidents in a variety of ways. Because each incident poses significant risk to the organization's ability to continue operations, this often leads to chaotic and reactive incident response.

Advancing to a structured, orderly response requires investment and planning – beginning with a risk-based approach to define and prioritize incident types. To achieve this, enterprise security teams require a strategy that drives preparedness, including standardization and testing of IR plans. Both are critical to reducing incident response times.

At this higher level, security organizations have a better sense of the company's primary line of business. Security leaders seek to understand and map the range of threats facing the enterprise. This allows security teams to craft plans that can respond to a range of cyber incidents and focus on minimizing disruption to keep the business going.

High functioning organizations test and improve IR plans at regular intervals. These incident response plans become the foundation for building an incident management program.

THE PATH FORWARD:

Develop an incident management program aligned to the needs of the business

Adopt a Risk-Based Approach

Security operations teams investigate events as standard operating procedure. Security incidents (one or more security events compromising critical or proprietary information or impairing business operations[2]) require action to minimize business disruption. IR teams verify security incidents based on understanding which data, applications and infrastructure are business-impacting. Aligning priority of security incidents to an Enterprise Risk Management (ERM) program helps focus response efforts.

Standardize

Business-aligned IR teams include a variety of technical and non-technical focused responders. "Table top" exercises provide an opportunity to assemble these combined teams at regular intervals. "Red team reviews" test and prepare the technical responders and forensics teams. Governance reviews help standardize:

- Roles and responsibilities
- Vendor MSAs
- Rules of engagement

Training based on IR exercises proves effective at teaching security awareness to employees.

Real world scenarios and rotational assignments of IR teams enable a cultural shift within the enterprise.

Orchestration is Key

Successful execution of incident response plans demands orchestration - the arrangement, standardization and coordination of all aspects of an enterprise-wide IR plan. Despite the availability of in-house capabilities and expertise, responding to a cyber incident often requires specialized skills. Due to resource scarcity and high cost, most organizations develop partnerships with one or more third parties. The orchestration of in-house and external resources provides the foundation to properly respond, remediate and recover.

Continuously Improve

Program governance spans beyond security and IT organizations. As IR plans include the entire business, testing is performed on a wider scale. Collecting, evaluating and integrating feedback from IR activities into security strategy and the incident management program fosters better preparedness. As organizations mature and become better prepared, less incidents rise to the level of "crisis."

CALL TO ACTION:

Take a stronger, broader approach to managing cyber security incidents

Today's enterprises need to prepare on a broader scale to endure a breach. Applying a programmatic approach to managing cyber security incidents demands the involvement of more than security teams. In the persistent effort to maintain brand integrity and profitability, a structured, well-orchestrated response to cyber security incidents supports a more resilient business.

1. Sources: 2011 Data Breach Investigation Report - http://www.verizonenterprise.com/resouces/executivesummary/es_2011-data-breach-investigations-report_en_xg.pdf
Sources: 2015 Data Breach Investigation Report - http://www.verizonenterprise.com/DBIR/2015/
2. Los Angeles Times. "Federal, state officials launch inquiries into Anthem data breach", February 2015. Retrieved from: http://www.latimes.com/business/la-fi-anthem-hack-20150206-story.html
3. Associated Press. "AP NewsBreak: ITS says thieves stole tax info from 100,000". March 2015. Retrieved from http://bigstory.ap.org/article/34539a748b3745ffb92451472f814ffa/apnewsbreak-irs-says-thieves-stole-tax-info-100000

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

12.15 | F1