protiviti®
Risk & Business Consulting.
Internal Audit.

Incident Response – Securing Executive Support to Address Security Breaches Effectively

POWERFUL INSIGHTS

Issue

The prevalence of malware in corporate networks is on the rise. However, with the continued commitment of malicious attackers to access valuable personal or financial information and the increased sophistication of malware used to accomplish such attacks, many organizations lack the process, technology and governance to combat this growing threat.

While prolonged malware attacks designed to collect valuable information are not new, the information security community has recently termed these ongoing occurrences as advanced persistent threats (APTs). Attacks of this nature often result in the compromise of multiple systems, the collection of mass data over time, and the transmission of such data to an attacker or attacker network.

Responding to a security breach is only possible with an effective incident response plan. This no longer is considered just a best practice, but also an obligation and demonstration of due diligence, especially for an organization that maintains sensitive data or personally identifiable information (PII).

There has been a dramatic increase in the number of companies that have experienced data breaches, many involving an APT, that did not have an effective incident response plan in place and suffered the consequences. As a result, a growing number of organizations want to improve their response processes.

Challenges and Opportunities

Successfully managing incidents or breaches includes preparation, the identification of the event, containment and minimization of the incident, and eradication of the incident. Yet one of the most important steps is the first one: gaining management support.

An organization can implement an incident response plan only with sufficient executive sponsorship. However, unless the organization has experienced an incident, executives often are reluctant to fund the development of a comprehensive program. Even in cases where regulations or industry requirements mandate a plan or program, organizations often succumb to several common pitfalls:

- Developing a plan "good enough" to satisfy the business and non-IT personnel of the organization
- Developing a written plan or program documentation but failing to implement plan dependencies or controls
- Failing to include an escalation plan, appropriate roles and responsibilities (specifically accountability for the plan's execution), and maintenance of the response program
- Testing just enough to demonstrate compliance but failing to test the plan thoroughly
- Failing to enhance plans, e.g., not evolving procedures to address evolving threats such as APTs
- Failing to evaluate the capabilities and culture of the environment and establish relationships with law enforcement and third parties to aid in response activities

Gaining executive sponsorship drastically reduces the likelihood of these mistakes.

Traditionally, few executive stakeholders (outside of CIOs, CISOs and CTOs) have been engaged in the implementation of incident response strategy. However, with state breach disclosure laws such as the Massachusetts Data Protection Law (201 CMR 17.00) and the adoption of industry regulations and standards such as the HITECH Act and PCI-DSS, business executives and those with corporate financial obligations are now more apt to support these initiatives.

Combined with recent media coverage of significant data breaches, security, audit and IT practitioners are in a strong position to gain the support required to implement an effective incident response program.

Our Point of View

Effective incident response processes are critical to the preparedness of companies to reduce the occurrence, proliferation and impact of a security breach. Key stakeholders should support the development of a plan appropriate to the organization's scale, culture, regulatory obligations and business objectives.

When soliciting support, stakeholders should stress the importance of developing a plan that:

- Integrates and complements existing information security programs – for example, an organization that has implemented government information security controls should consider incident response procedures consistent with NIST 800-61.
- Includes input from various stakeholders – compliance, IT, security operations, corporate security, corporate communications, regulatory and legal affairs, etc.
- Includes clear direction and core processes that are followed in the event of an incident.
- Clearly assigns roles, responsibilities and accountability to groups or offices within the organization.
- Includes escalation paths and communication procedures to ensure appropriate stakeholders are involved in key decisions pertaining to response and disclosure.
- Is complemented by procedures that provide instructions regarding actions to take in response to specific types of incidents. For example, the method of responding to a distributed denial of service attack varies greatly from the method of managing a malware incident.
- Is kept current, i.e., is evaluated at least annually.
- Addresses regulatory obligations regarding incident response or breach disclosure.
- Ensures appropriate parties maintain key contacts in law enforcement and the media to expedite actions as dictated by the organization.
- Ensures trusted and qualified parties are available should the scope or specifics of the incident exceed the resource availability or capabilities of in-house personnel.
- Considers, if an incident occurs, the potential duty to preserve relevant information and evidence; potential legal and regulatory actions; and costs, time and burden of e-discovery.

PROVEN DELIVERY

How We Help Companies Succeed

Protiviti has deep expertise in response execution, forensic analysis and response plan development. This expertise has resulted from our years of experience and dedication to the development and enhancement of world-class incident response practices. We are recognized as a leading provider of Incident Response and Forensic Services by the PCI Standards Security Council.

Our Incident Response and Data Forensics Investigation services include framework/program development as well as support services. We serve numerous clients around the globe on both an advisory and 24x7 retainer basis.

Example

Protiviti responded to a breach of personal financial information requiring the deployment of response and forensic resources nationally. We were responsible for system analysis, malware analysis and the evaluation of logs and other system records to determine the cause and extent of data compromise. We identified all systems impacted by the APT, developed and implemented a containment strategy, and prevented the further compromise of financial data. We also assisted our client in fulfilling breach notification and reporting requirements.

In addition, our efforts and intelligence were invaluable to law enforcement agencies, which were able to take action against the entity responsible for the security incident.

Contacts

Rocco Grillo
+1.212.603.8381
rocco.grillo@protiviti.com

Frank Wu
+1.213.327.1509
frank.wu@protiviti.com

Joseph Rivela
+1.212.399.8657
joseph.rivela@protiviti.com

About Protiviti

Protiviti (**www.protiviti.com**) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. The firm helps solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Protiviti's highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

protiviti®
Risk & Business Consulting.
Internal Audit.