Data Breach Recovery

Overview

Emagined Security helps successfully guide clients through data loss, security breach incidents and forensic investigations. By using highly efficient methodologies, Emagined Security helps minimize the internal and external pressures associated with publicized data breaches, and gives management reasonable justification for data loss prevention and security budgeting.

The goal of Emagined Security's data breach recovery services is to first and foremost react appropriately to a current incident, analyze, scope and remediate the root cause, and then prevent the breach from recurring through audit and control methods using a five-phase approach.

Benefits

By using Emagined Security your organization gets the positive effects of:

- A superior quality, ethical organization: Emagined Security is well known and is highly regarded
- Priority and Professionalism: Your breach incident is treated in a confidential, professional manner, with your data, information and its security as the highest priority
- Identifying and managing risks to help reduce the risk of another or further damaging exposure
- Risk Reduction: Reduce the risk to your organization, through lost revenue and data, of an additional data breach
- Risk Management: Improve Governance and corporate strategy of privacy and security risks
- Risk Identification: Obtain a complete and accurate view of sensitive and personal data in your organization
- Risk Control: Obtain an auditable risks list and associated controls
- Report-ability: Providing your Board with reasonable assurance that risks were evaluated and managed
- Due Diligence: Fulfilling due diligence requirements for both internal and external parties

Description of Service

Emagined Security's Data Breach Recovery services revolve around the five-phase approach, which includes the Triage, Assess, Prioritize, Remediate, and Maintain & Audit methodologies.

Phase 1: Triage - React Appropriately and with Alacrity

The Triage phase begins with a discovery session and security assessment. The Triage Team will work closely with the identified Incident Response Team during the incident and will expect to use deliverables

from members as a foundation for the triage efforts. The Triage phase ends when the Triage Team is confident that the root cause has been identified and properly remediated.

Phase 2: Assess - Identify Remaining Threats & Vulnerabilities

The Assess phase is characterized by conducting a thorough Security Assessment. The Security Assessment provides an organization with a fresh look at its current threats and vulnerabilities from a third party, neutral perspective. The Assessment can include:

- An evaluation of existing network security architecture, policies and processes, based on the globally recognized standards and industry best practices
- An assessment of the current vulnerabilities on the network and its hosts
- Interviews & walkthroughs with key staff members in IT
- Interviews & walkthroughs with key staff members from the Business

Phase 3: Prioritize - Determine Optimal Combination of Spend vs. Risk Reduction

Side-by-side solution analysis & project prioritization with key staff members from both the Business and IT is needed to develop actionable recommendations and the detailed remediation plan required to achieve the desired improved security state. Emagined Security will work closely with your team and will assist in presentation of assessment results and action plans to executive, management, and staff audiences. Executive management will feel increased confidence that the analytic and data driven remediation plans will provide adequate risk reduction with optimal levels of budget.

Phase 4: Remediate - Reduce Business Risk by Closing Gaps

Ongoing monitoring, management, and tracking of remediation items through closure is required to close out issues identified during the Security Assessment. Remediation activities frequently require more resources than anticipated and some prioritization can be used to quickly and effectively remediate and mitigate the issue(s). Leveraging teams with prior experience in successfully managing remediation projects is where efficiencies can be realized.

Phase 5: Maintain & Audit - Prevent Re-Occurrence Through Effective Governance

Once remediation projects are completed maintenance becomes necessary. An improved control environment to prevent re-occurrence of issues must be implemented. The organization's overall IT Governance posture will be improved in its ability to identify, measure, and remediate newly identified current and future risks.