Marshall Eddy

CS331-001

Vincent Skimmer

24 October 2016

Risk Management

The first step in assessing an organization’s cyber risk is to understand what company assets you are trying to protect and why. Ask yourself, what are your most critical assets?  Identify your most important information, assets, and legally protected information. Some ways to help identify your biggest threats are by asking (and answering) the following questions: how do you store the information, who has access to the information, how do you protect your data, and what step are you taking to secure your computers, network, email and other tools (staysafeonline.org). A comprehensive cybersecurity plan needs to focus on three key areas: prevention, which are solutions, policies and procedures need to be put in place to reduce the risk of attacks; resolution, in the event of computer security breach, plans and procedures need to be in place to determine the resources that will be used to remedy a threat; restitution, companies need to be prepared to address the repercussions of a security threat with their employees and customers to ensure that any loss of trust or business is minimal and short-lived.

Avoiding a cyber crisis often comes down to properly managing a cyber incident before, during, and after it unfolds. This starts with a broad view of cyber crisis management. Executives often see cyber incidents as “an IT issue,” when IT is only one domain involved. Forward-thinking management teams recognize that effective crisis planning involves multiple functions and skill sets. They also recognize that these must be highly coordinated if an incident is to be contained or, if an incident does escalate to crisis levels, managed (www2deloitte).

Readiness equates not only to vigilance, for example in the form of 24/7 Monitoring, but also to readiness of resources. A well-prepared, multifunctional team must be poised to deal with all aspects of an incident or crisis. In addition, crisis simulation and war gaming enables management to understand what can happen, which steps to take, and whether the organization is truly prepared.

Management’s response can either contain or escalate an incident; indeed, a poor response can even create a crisis. Vigorous, coordinated responses to incidents limit lost time, money, and customers, as well as damage to reputation and the costs of recovery. Management must be prepared to communicate, as needed, across all media, including social media, in ways that assure stakeholders that the organization’s response is equal to the situation.

Immediately after an incident, affected capabilities must be restored. This usually takes hours or days, but can take weeks or months in severe cases. Also, cybersecurity must be enhanced to secure the environment, improve visibility into threats, and reduce the impact of future incidents. Containing an incident and avoiding a crisis calls for proactively addressing stakeholder concerns. Customers usually express concern regarding loss of personal data and privacy and may develop long-term brand aversion.

Business partners are concerned about near-term cross-contamination of their systems and the longer-term integrity of data and transactions. Employees may be overwhelmed by negative publicity and increased stress. Regulators want assurance regarding consumer protection, and the state of the business and industry. Investors are attuned to short-term financial impacts and longer-term business and brand viability.

Over the course of the response lifecycle, crisis communications stand among the highest priorities. Specifically, the organization must: Respond to a high volume of requests from customers, business partners, vendors, regulators, law enforcement, and the board of directors. Manage requests from business partners to modify arrangements, processes, and methods of sharing information. Engage in proactive messaging to the broader base of stakeholders and the public regarding what is known and not known, and what the organization is doing. Monitor and address traditional, web based, and social media reactions to the event and to the organization’s response and intentions In addition, management must: Address any potential threat of legal or regulatory action, and determine what legal recourse is available to the organization. Minimize the time between developing and implementing the remediation plan, while also managing the risks generated in that interim The more comprehensive and tested the plan, the better management’s response to an incident will be. Yet management should understand that the plan does not represent a script that will play out in reality and that responses must be flexible and fluid. You may have to depart from the plan, but the plan will provide a framework and guidance for coordinating the diverse elements involved in the response.

References

www2.deloitte.com

staysafeonline.org