RIMS the risk management society

Professional Report

CYBER PROTECTION: WHAT TO DO BEFORE AND AFTER A CYBER INCIDENT

Cybersecurity is now a critical component of corporate governance. According to a report released earlier this year by CyberScout and the Identity Theft Resource Center, the number of data breaches reported in the United States in 2016 increased by 40% from the prior year to a record 1,093 incidents that exposed 36 million records. The business sector had the highest number of disclosed breaches with 494, followed by health care at 377, education with 98, government with 72 and financial institutions at 52.[1] Globally, the cost of cybercrime is expected to reach $2 trillion by 2019, an increase of 300% from the estimated $500 billion cost in 2015.[2]

From an enterprise risk management perspective, there are several protocols that every business should have in place both for prevention of data incidents and handling an incident if one does occur. A strong partnership between IT, legal, risk management and public relations is critical for a strong cybersecurity program.

PRE-INCIDENT PREVENTION

Prior to a cyber incident, the risk manager should work with key organizational stakeholders to identify and assess the organization's risk. Know what data the organization holds and where it is in the organization to understand its value and vulnerability. Monitor the external environment for emerging threats, including those which may be specific to your industry. If your organization purchases cyber insurance, the insurance application itself can be a valuable tool for assessing the organization's risk.

In addition to maintaining an IT environment that is resistant to cyberattacks with current software and protected system access points, there are several activities that can be undertaken to reduce the ability for hackers to gain access to an organization's information and reduce the impact should an attack occur.

Employee training and periodic testing are as important as the most current security software. Employee carelessness can bypass the most stringent security firewall and allow access to data or an opportunity for ransomware to penetrate a system. Are regular training and reminders to be cautious with emails from unfamiliar sources an on-going part of your cybersecurity program? Are emails originating from outside your firm clearly identified in the body of the message? Do you have a process in place to capture outgoing emails for review, such as those containing large amounts of employee data or providing wire transfer information?

One in 131 emails contains malware, according to a recent study by Symantec. It is estimated that over 400 businesses are targeted each day, with $3 billion lost over the past three years.[3] It is very common for criminals to use the name of a senior executive with an email address very similar to a company's URL to request wire transfer of funds or employee data that can easily be overlooked by an employee. Something as simple as a red banner identifying e-mails

from external sources can be effective in preventing employees from opening e-mails containing malware, responding to requests to send money or sensitive employee data to criminals "phishing" for information.

While insurance is not a panacea, every organization should consider purchasing a cyber insurance policy. According to the Ponemon Institute, the average cost of a breach in the United States is $7 million.[4] Therefore, it is important to take an active role in the development of your cyber insurance program and understand what is covered. Coverage and services can differ widely, but many offer crisis management and response services that can be invaluable in the event of an incident. The applications can be arduous, but will help identify strengths and weaknesses in your cybersecurity program. Some insurance packages also offer risk management tools, such as employee training packages. Collaboration between IT, risk management, legal, and your insurance broker or agent in the evaluation of competing programs will help develop a program that is tailored for your particular situation. Coverage can include the cost for notification of the incident, identity theft protection for affected parties, third party lawsuits and extra expenses for public relations work.

You should also check other policies for cyber coverage. For example, property policies may include coverage for damage caused by machinery malfunction as a result of a system intrusion. Understand what constitutes a coverage trigger under your policies and any exclusions. Identify these before an incident so that the organization can be in the best claims posture post-incident.

Develop relationships with law enforcement including local police, the FBI and Secret Service, before they are engaged in an investigation on your behalf. Data incidents should be reported and if law enforcement knows your team and your exposures, it will make reporting much easier. Law enforcement can also help with employee training and communication.

Work with your insurance carrier to choose a law firm in advance with cyber experience. Not only will you need specific legal expertise to defend any claims that might arise from an incident, you will also need legal assistance in reporting a cyber incident. There are 49 separate state requirements for breach reporting with specific requirements for reporting thresholds, timeframes, forms and notification requirements. The time limit for reporting can be very short and many states have very specific requirements for notifying affected parties, with fines for non-compliance. A law firm knowledgeable in these requirements can save time, money and frustration with compliance requirements.

Select a public relations firm experienced in crisis response. If you purchase cyber coverage, check with carrier on their resources. Most insurers will include the cost of this service in their policy and will have identified reputable firms you can choose from to help with your situation.

Have a written IT disaster recovery plan and an organization-wide crisis management plan in place and test it on a regular basis. The plans should provide clear direction on responsibilities for dealing with an incident from a public relations standpoint as well as technical details. Clear communication is critical; lack of a clear concise plan for dealing with affected individuals, employees and the media can have very negative ramifications for brand and reputation.

POST-INCIDENT RESPONSE

Once an incident occurs, there are several best practices to help minimize the impact on your organization. One cannot emphasize enough the importance of current disaster recovery and crisis management plans that have been tested and where the team clearly knows their roles and responsibilities. One overall best practice, work with your legal team to protect internal communication under attorney client privilege to avoid these from becoming discoverable in the event of litigation.

Once a data breach, phishing, ransomware or other incident has been confirmed:

1. Ensure that IT is containing the issue and executing the disaster recovery plan to minimize the impact on the organization.
2. Inform your selected law firm immediately so they can begin review of the notification requirements in the affected states in a timely manner.
3. Notify law enforcement.
4. With the assistance of the public relations team, begin drafting an initial press release, FAQ and Q&A for impacted parties.
5. If you have cyber insurance coverage in place, notify your carrier and begin working with them to access the resources available under the policy.

Preserve evidence, but do it safely and isolate it to prevent further damage. Ensure that all traces of the hacker have been removed and any security lapses addressed. E-mails that may have been the source of the intrusion will be useful in forensic analysis and for law enforcement investigations. Evidence is also critical for investigation of the root cause.

To respond to questions from stakeholders impacted by the breach, activate the internal call center as soon as you have established your plan of action and have FAQs and Q&A ready for respondents. A prompt response to affected parties that includes clear communication and immediate remedies, such as identity theft and credit protection resources, will help preserve brand and reputation.

Having a clearly defined strategy to respond to cyber issues, that includes both incident prevention and post-loss response, will greatly minimize the financial and reputational impact of a data incident on your organization.

The RIMS External Affairs Cyber Security Task Force is:

TERI COTTON SANTOS
Senior Vice President, Chief Compliance and Risk Officer
The Warranty Group

DWAYNE EASTWOOD
Manager, Risk Management
McCoy's Building Supply

MICHAEL GRESHAM
Risk Manager
Half Price Books, Inc.

JOHN HANSEN
Vice President, Enterprise Risk Management
Sprouts Farmers Market

[1] ITRC Data Breach Report (Identity Theft Resource Center, January 19, 2017)
[2] Bill Laberis, 20 Eye-Opening Cybercrime Statistics (Security Intelligence, November 14, 2016)
[3] Symantec Corporation, Internet Security Threat Report (Volume 22, April, 2017)
[4] Ponemon Institute and IBM, Cost of Data Breach Study: Global Analysis, (June 15, 2017)