TRAVELERS
Prepare and Prevent - Cyber Risk Pressure Quiz

I took the Cyber Risk Pressure Test and
a pressure point in my cyber risk management strategy may be:

Response & Recovery

What does this mean?

35%

of users found that Response & Recovery is a pressure point in their cyber risk management strategy

When a suspected data privacy or security incident is reported, an organization must quickly initiate and manage their response. That takes planning. The high stakes process can be complex and stressful because a cyber attack or data breach can put your most sensitive information and critical systems — and even your reputation and bottom line — at risk. You must be prepared to respond quickly while addressing consumer inquiries and compliance issues. A comprehensive, cross-functional, detailed cyber incident response plan can help mitigate some of the risk associated with a cyber attack or data breach, while taking the uncertainty out of your recovery efforts.

Be Prepared

There are many things you can do in advance of an incident to help minimize or contain the damage of the breach or attack. Begin by assessing your data security gaps, then establish a framework for action where key decisions are made ahead of time - not under pressure. Have your cyber incident response plan address the following:

- Backup and storage of critical data, documentation and systems.
- Physical access to server rooms, critical machines and systems.
- Network activity monitoring and early detection of potential incidents.
- Data breach or incident validation procedures.
- Documentation of all investigation and mitigation efforts.
- Incident response team identification, training and activation.
- External resources, including your agent and insurance carrier, required to assist in the response and recovery process.
- Specific actions to be taken to mitigate the impact of a cyber attack.
- Data owner and customer notification protocols.
- Data recovery and restoration procedures.
- Post-incident "lessons learned" discussions and plan refinement.
- Plan testing and employee training.

Respond Quickly

Your immediate actions in response to a cyber attack or data breach may be the key to your ability to successfully recover. Here are nine things to consider doing immediately after an incident has been confirmed.

Contact Your Agent And Notify Your Insurance Carrier

Inform them that you believe an event has occurred.

Assemble Your Core Incident Response Team To Investigate And Monitor The Breach

The response team should also establish a communication protocol with critical internal and external resources.

Confirm Your Priorities

Ensure your team does everything it can to prevent harm to customers, protect your reputation, regain customer trust, prevent revenue loss, avoid regulatory fines and minimize recovery costs.

Contain, Fix and Restore

Identify the scope and root cause of the incident, and take the necessary actions to prevent it from causing further damage.

Engage Pre-Selected External Resources

Reach out to identify external resources for support in the recovery (legal, forensic, notification, PR, victim protection, etc.).

Seek Legal Advice

Immediate consultation with legal counsel may help you to understand and map out what needs to be done in response.

Ensure Compliance

Regulations such as the Gramm-Leach-Bliley Act and the HITECH Act have specific requirements for when to notify individuals, the media and regulatory agencies of an attack or breach. So do some individual states. Know them, and report to federal and state agencies in accordance.

Set Up A Call Center

Establish where and how to handle customer relationship management through the incident, and consider seeking outside assistance if necessary.

Prepare For An Investigation

Lawmakers are cracking down on cyber attacks and data breaches. Anticipate and prepare for regulatory requests and ensure vendors can support you during the investigation.

Understand the Risks - and Costs

According to recent studies, the top cyber risks that could leave businesses of all shapes and sizes vulnerable to attacks and data breaches include:

Human Error

Lost and stolen laptops and smart phones add up to big losses for companies.

Hackers

Someone outside the organization who gains unauthorized access to the network and steals information.

Spear Phishing

Social engineering targeted at employees often results in security breaches.

Extortion

An attack (or threat) against an organization, accompanied by a demand for money to stop the attack.

Hacktivism

Social and politically motivated attacks against commercial websites.

Rogue Employee

Someone who deliberately sends an email containing private customer information.

As the type and frequency of cyber attacks grow each year, so do the costs to resolve a data breach. The average number of records lost in a cyber breach has reached 30,000[1], which can cost a business a significant amount to resolve, including:

- Average notifications costs: $500,000[1]
- Average post breach costs: $1,600,000[1]
- Average lost business costs: $3,300,000[1]

- Average detection costs: $400,000[1]
- Average defense and settlement costs: $800,000[2]

Imagine your business or organization needing to cover these types of expenses — that is why being prepared and protected is a necessity for any business that uses technology today.

Sources
[1]Ponemon 2014 Institute Cost of Data Breach Study
[2]NetDiligence 2013 Cyber Liability & Data Breach Study

Suggested Reading

- How to Develop an Incident Response Plan
- Business Continuity for Data Management
- Cyber Security Tips
- Cyber Insurance Solutions
- Securities & Exchange Commission - Cyber Guidance

Remember: No Business is Immune to Cyber Risk

Take this as an opportunity to turn your organization's cyber risk challenges into business advantages. Consult with your company's risk management advisor and insurance agent/broker to better assess which points in your organization may be vulnerable, then work together to prepare for a potential threat and plan for a quick recovery.

Take the Cyber Risk Pressure Test

View My Results