E-COMP NOW!
Business Insurance Simplified

Recovering from a breach

Learnings from real incidents at Small and Mid-size Businesses

2019REALINCIDENTSAREGOODEXAMPLESOF WHATITTAKESTORECOVERFROMANINCIDENT

[N*ote: the information below is pulled rom the public ITRC (Identity Theft Resource Center) database which maintains a public list of cyber incidents. This document only refers to publicly available information.*]

BelowisalistofSMBsthatfellvictimofadatabreachin2019.Thisshowsthat:

1. Regardless of size and class of business, no business is immune to cyber incidents
2. The damages resulting from a cyber incident are multi-facetted. From technical security experts to lawyers or credit monitoring, it is easy for anybody who has not experienced a breach yet, to underestimate the amount of work required to return to normal operations after an incident.
3. Cyber liability insurance not only provides coverage for the expenses related to a cyber incident but also provides immediate access to vendors and experts that can help a business recover and navigate the stressful event.

INDUSTRY: SERVICES

Email compromised at building cleaning service company (500 employees, $15M of revenue)

An unauthorized individual gained access to several employees' email accounts.

As specified in the **breach disclosure communication to customers**, the company had to make significant investment to understand the scope of the incident and which type of data was compromised.

- Incident: Unauthorized access to an email account might have compromised personally identifiable information.
- Post breach activities: Incident investigation to identify impacted customers, notification to all customers, complementary one-year credit monitoring for all customers impacted.

INDUSTRY: MANUFACTURING

Website attack at $10M industrial bakery with 145 employees

Through the use of malicious code, an unknown third party gained unauthorized access to the company website.

According to the **data breach notification letter sent to impacted parties**, unauthorized access could have lasted for 22 months before being discovered.

- Information compromised: Customer names, payment cards, expiration dates and security codes.
- Notifications: Customers, law enforcement, payment card companies.
- Disruption: Ordering and account login on the company website was disabled while improvements including the platform supporting the site were upgraded for security.

INDUSTRY: ENTERTAINMENT/HOSPITALITY

Email compromised at Health Club with <$10M of revenue & 120 employees

Through the use of malicious code, an unknown third party gained unauthorized access to the company website.

This mail notification highlights the **steps taken post breach to notify impacted customers** and employees.

- Information involved: Customer names, payment cards, expiration dates and security codes.
- Notifications: Customers, law enforcement, payment card companies.
- Disruption: Ordering and account login on the company website was disabled while improvements including the platform supporting the site were upgraded for security.

INDUSTRY: ONLINE RETAIL

Compromised website at a $30M business with 30 employees

Through the use of malicious code, an unauthorized person gained access to the payment card information entered by customers on the website. In the data breach notice, the company offers one year of identity protection services amongst other services.

- Information compromised: Customer names, payment cards, expiration dates and security codes.
- Post breach activities: Notified law enforcement and launched an incident investigation in cooperation with them. Engaged a third party expert to review company's security protocols.
- Measures taken: Offered one-year complimentary subscription to third-party identity protection and restoration services and credit monitoring; set up a hotline for all customer's inquiries regarding the incident.

INDUSTRY: HEALTHCARE

Phishing email attack at healthcare provider with less than $50M in revenue

This medical center was victim of a phishing email attack.

The notice of data breach published on their website describes what happened and actions taken to remediate the incident.

- Post breach activities: Engaged outside experts to investigate the incident and determine the full nature and scope of the breach, ensure systems are secure and identify "(through a very tedious technical assessment and hand document review process)" the exact emails that were actually acquired by the unauthorized third party.
- Measures taken: Offered complementary identity theft protection services to potentially impacted accounts. Established a toll-free hotline to answer any concerns or questions related to the incident.
- The organization is also taking steps to enhance its security and prevent future incidents.

The above cyber incidents are just a small sample. The hardship caused by cyber incidents can extend to every aspect of a business and include:

- Operational downtime
- Costs of finding what systems, data, or accounts were impacted by the attack
- Cost of notifying customers and employees whose data might have been compromised
- Lawsuits from these customers
- Costs of removing any malware and repairing systems
- In the case of credit card compromise, cost of providing credit monitoring services for impacted individuals
- Regulatory fines if protected data has been compromised
- Lost business because the business' reputation has been tarnished.

HOW CYBER INSURANCE CAN HELP:

Cyber insurance is designed to protect businesses from risks related to the use of computers, connected devices, applications and the internet. Such risks are often excluded, insufficiently covered, or too vaguely defined in general commercial liability policies or business owner policies (BOPs) .

Based on the unexpected losses and expenses identified in the examples above, cyber insurance should include first-party coverage to cover direct losses such as data destruction, theft, or hacking and third-party liability coverage to cover for the damages or losses caused to others. Cyber policies should also broadly cover expenses that occur in the aftermath of a cyber incident to enable the business to come back to normal operations as quickly as feasible.