CYBER, SECURITY & PRIVACY »

RT ProExec

CROSS INSURANCE

New England Community Action Partnership

Connecticut | Maine | Massachusetts | New Hampshire|Rhode Island | Vermont

NECAP New England Community Action Partnership

May 18th, 2017

This presentation is advisory in nature and all examples and descriptions are for illustrative purposes only. Whether or not or to what extent a particular loss is covered depends on the specifics of the loss and the terms and conditions of the policy as chosen.

RT ProExec

“It’s not a matter of *if* but of *when*”

Over the last year, a record high 4.2 billion records were compromised due to data breaches

This is a large increase over the previous all time high of 1 billion records compromised in 2013.

Criminals can use stolen information such as social security numbers, addresses and names to file false tax returns, order credit cards and to siphon money out of consumers’ bank accounts

RT ProExec

Can this happen to me?

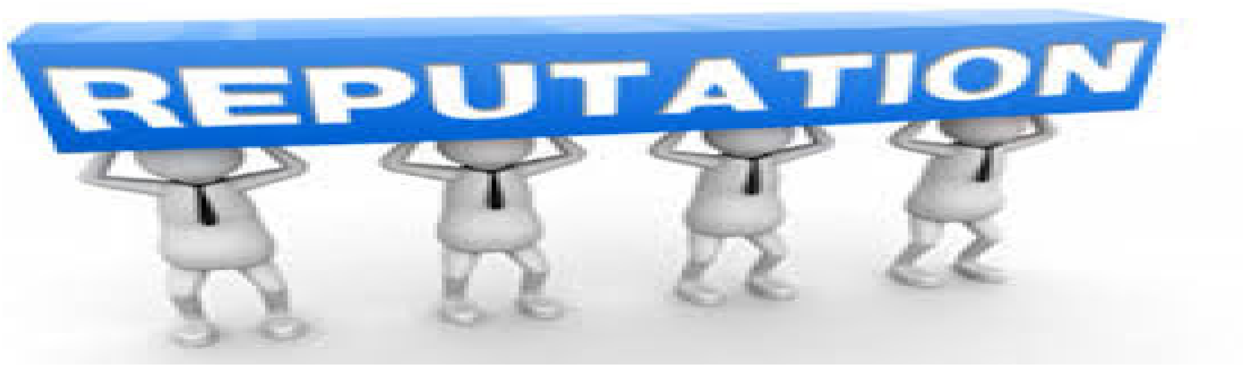
- 59% of employees steal proprietary corporate data when they quit or are fired.
- Four out of five victims [of a breach] don’t realize they’ve been attacked for a week or longer
- 30% of phishing emails are opened. And about 12% of targets go on to click the link or attachment
- 80% of analyzed breaches had a financial motive
- The forecast average loss for a breach of 1,000 records is between $52,000 and $87,000
- The cyber insurance market—mainly a U.S. market—has grown from $1 billion to $2.5 billion over the past two years, and it is expected to grow dramatically and expand globally over the next five years

What is my legal responsibility?

The patchwork of breach notification laws now exist in 48 US states and provide a great deal of exposure for all industry types. These laws prioritize the security of financial information and in the event of a data breach, require costly internal investigations, significant expenses for breach vendors and hefty regulatory fines & penalties

RT ProExec

What will my customers think?



The publicity fallout from a data privacy breach entails the risk of massive reputational and brand damage. It is safe to assume that poorly handled breaches result in far higher customer defection rates; in fact, brand value and reputation have been shown to decline by between 17% and 31% after a mismanaged breach, and it can take upwards of a year to restore an organization’s reputation

I have heard the term Cyber Liability before, but what are these policies really covering?

Unfortunately, many insurance carriers differ in not only the coverage they are providing, but also the terminology of their policy language. This creates much confusion among policy holders and major concerns about how their policy will respond when a breach occurs.

Third Party Liability Coverage

Network Security Liability

Provides coverage for actions that the insured is legally liable for such as hacking, system intrusions, unauthorized access, release of malicious code, denial of service or DDOS attack

Privacy Liability

Negligence in protecting and/or failure to safeguard confidential data, disclosures of confidential information, breaches of confidentiality, failure to comply with breach notice laws, violations of privacy laws/regulations, privacy regulatory actions

Website Media Liability

Provides coverage for actions that the Insured is legally liable for claims made against the Insured for a Media Peril of content on the Insured's Internet Site. Copyright Infringement, Defamation, etc

Mental Anguish

Provides coverage for the emotional trauma one may endure due to a privacy breach or network security event

Regulatory Coverage

Provides coverage for actions/ proceedings and fines/penalties against the Insured by a regulatory agency resulting from a violation of a Privacy Law

The Anatomy of a strong Cyber Policy

RT ProExec

First Party Coverage Expenses

Network Interruption Business Income & Extra Expense Coverage

Provides coverage for the Loss of Income and expenses incurred to reduce Loss of Income, minimize the duration of a Network Interruption, Forensic Expenses, Loss of Data due to a Network Attack/Denial of Service Attack.

Cyber Extortion Coverage

Provides coverage for costs and expenses related to a Cyber Extortion Threat, including a threat of a Denial of Service Attack, Dissemination of Private Information obtained though the Insured's Computer System, alter/delete/damage Data or a Data Asset or the Insured's Computer System or interrupt/suspend the Insured's Computer System unless money or other valuable consideration is paid by the Insured

Breach Notification Forensics & Credit Monitoring

Covers costs & expenses associated with the notification to individuals whose Personal Identifiable Information or Protected Health Information has been breached due to federal, state or foreign Breach Notification laws. Such covered services include forensics, legal services and credit monitoring.

Crisis Management Coverage

Provides coverage for costs and expenses incurred by the Insured for a public relations firm, law firm or other expenses to communicate with the general public in order to mitigate reputational damage

Data Loss Coverage

Provides coverage to restore data due to a network security breach.

Top five ways to assist in avoiding a breach

1. Encrypt your devices

Encryption is a safe harbor under virtually every breach notification law.

2. Automate patch management

Staying on top of the latest available software patches and moving to automated patch management can protect against a breach.

3. Enforce password complexity

Computer systems can now systematically cycle through all permutations of potential passwords.

Don't use "bad" passwords that are easy to crack ... dictionary words are capable of being deduced with an algorithm.

4. Be alert to phishing

Most breaches occur because of human error. Training is a critical step in breach preparedness. It is important to train employees to spot the indicators of a phishing email.

5. Double check before hitting send

It may be simple, but double-checking the contents of a file, email address or mailing details can really save - especially when sending data to outside vendors.

RT ProExec

Claim Scenarios

Incident Type: Hacking/Malware (phishing)

Description: The insured's systems were potentially compromised due to a spear-phishing scheme that resulted in a fraudulent wire transfer and potential exfiltration of emails with customer PII. BBR Services recommended forensics and privacy counsel, and they concluded (after an extensive manual review of data) that the insured was legally obligated to notify approximately 3,000 individuals.

Incident Type: Stolen Portable Device (unencrypted)

Description: An employee had an unencrypted laptop stolen from her automobile. BBR Services quickly connected the company with forensics to assist with assessing the information on the laptop. Once that analysis was complete, the organization learned that the laptop had contained protected information on approximately 6,000 individuals. BBR Services continued to assist by coordinating notification and call center services, as well as credit monitoring, for the affected individuals since the laptop contained their social security numbers.

Incident Type: Hacking/Malware

Description: An insured discovered malware on the majority of its computers. The company’s HR director’s account was accessed and money was electronically transferred from a bank account. All 140,000 members were notified and offered credit monitoring.

Incident Type: Missing Portable Device (unencrypted)

Description: Insured discovered two backup tapes missing. Forensics evaluation uncovered the tapes contained PII for 84,000 individuals. BBR Services coordinated a response, including notification and call center services.

Incident Type: Hacking/Malware

Description: A bank experienced a sophisticated malware attack, where hackers were in the insured's system for at least six months. The hackers set up fake accounts and money was withdrawn from the bank from those fake accounts. The forensic investigation was extremely expensive due to type of malware. Together with BBR Services, the bank notified and provided credit monitoring to about 30,000 individuals whose credit card numbers, SSNs and driver's license numbers may have been exposed.

Incident Type: Inadvertent Disclosure (email)

Description: A credit union employee inadvertently sent an email to a third party outside the company which contained credit union member names, account numbers and social security numbers. Approximately 650 members were affected, half of which included SSNs and the other half included just names and account numbers.

Questions?