MCB MARCIA C. BROGAN Insurance Agency, LLC. Business | Personal | Childcare

WNY @ WORK WHERE IDEAS & SUCCESS COME TOGETHER ESPN 1520AM

Insurance Nightmares: EXPOSED!

September 22 , October 13- 2019
Guest: Christopher Goss, Vice President Philadelphia Insurance New York

What is cyber liability, why is it important, what is the chance of a business needing it and how will it protect my business?

Cyber is one of the most prevalent threats facing businesses today and the products and processes that businesses need to heed can be the difference of a business surviving the compromise or closing their doors

Cyber Liability is an exposure of any data and information on equipment that is owned by you or leased to you that contains information about your employees, customers, clients or businesses. Cyber coverage can also cover recreation or restoration of files, public relations, regulatory notifications, credit monitoring and fines and fees. .

Any business can be breached with the smaller to midsize company being the most vulnerable because they might lack the resources to secure their environment.

60 % of small business close their doors after they have been compromised. Average cost is $385,000 for small businesses. $157 per record to repair.

Why Small Businesses?
Small business are prone to attacks from Ransomware with the going rate for a small business to pay to receive the release code is about $5000. Hackers know that that FBI focuses on large companies that have a high exposure (SONY, Target and that the FBI does not have the staff to investigate small threats.

In order to have the FBI investigate the attack the company needs The FBI will not investigate claims of that size because due to limited staffing they need to focus on large attacks like Target, SONY etc. The attackers know that and keep the ransom that amount so they are under the radar but if not paid it could force the small business to shut down. A senior underwriter with Tokyo Marine (Business Insurance America Magazine Sept 2019) states that the trend is shifting to smaller companies like doctor's offices in order to make a quick $5000-$10000.

IBM reported that the largest sectors compromised were:

- Financial services companies include banks, insurance, investment management, brokerage and payment processors.
- Industrial and manufacturing companies
- Technology and retail.

U.S. was the highest in frequency of attacks with 14 % out of the 15 country's represented in the study.

Examples of compromises:

- Ankle and Foot Center of Tampa 156,000 records were hacked
- 21st Century Oncology: 2.2 million records were hacked
- Ancestry.com: 300,000 due hacked due to poor security
- AT&T: 113,000 records due to a lost or stolen computer
- Embassy Cables: 118,000 records due to an inside hack
- Facebook : 6 million due to it being accidentally published
- Hyatt Hotels : 250 locations were hacked
- Target: 110 million were hacked
- TJ Max 94 million were hacked

In 2019, a collection of 2.7 billion identity records, consisting of 774 million unique email addresses and 21 million unique passwords, was posted on the web for sale.[4]
https://en.wikipedia.org/wiki/List_of_data_breaches

Some types of compromises are:

Internal threats:

- Phishing- employees clicking on malicious links,
- plugging in from infected drives
- divulging configuration details over the phone to outside sources
- rogue employees

External threats

- ransomware
- malware infection.

I use a hosting company aren't I protected?

- The hosting company may or may not have cyber insurance. If they do , insurance will make that hosting company whole first, then then the insurance company will work with hosting customer base starting with the biggest customer and so on down the line. There may or may not be coverage for all the compromised customers. The hosting company's customers have customers and those customers who were compromised are left feeling the pain and violation of the attack- which is a public relations nightmare.

What does insurance cover when you have a claim:

- Detection include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors.
- First and third party
- May include paper breach as well as cyber
- Notifying the victims
    - These costs include help desk, communications, special investigative activities, remediation, legal expenditures, identity protection services and regulatory intervention also include costs that relate to communication with data protection regulators and other related parties.
    - The United States had the highest notification costs due to numerous regulations requiring disclosure to data breach victims and regulators.
    - Activities that attempt to minimize the abnormal loss of customers as a result of the data breach event, the cost of new customer acquisition following the disclosure of the data breach, costs relating to business disruption and revenue losses. Public relations
- Safeguard Suggestions:
    - Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimize potential harms.
    - Redress activities such as credit report monitoring or the reissuing of a new account (or credit card).

Regulatory fines and penalties are not allowed to be insured and those fees and fines can start over $100,000.

New Legislation:

- Governor Cuomo signed the “Shield Act” (Stop Hacks and Improve Electronic Data Security) which imposes stronger obligations on businesses handling private date to provide proper notification to affected consumers where there is a security breech.

Costs:

- Insurance costs vary depending on exposure (number of employees, data, information gathered etc) and start at $1000.00
- By not having the proper insurance safeguards which offers a team of knowledgeable professionals who will work with diligently to defend and protect your business
- If the business owner is not aware of the scope of the breech and the requirements they may not fail to comply with the guidelines therefore means higher costs, fines and finally will need to engage consultants which would increase post data breach costs.

Reference: https://www.ibm.com/downloads/cas/4DNXZYWK

What can businesses do to protect their business:

- Invest in governance, risk management and compliance programs
- Evaluate risk across the organization and track compliance to improve an organization's ability to detect a data breach.
- Have the right protection and existence of a strong incident response team that can be provided by the insurance company! Quick action can result in an average decrease in the per capita cost of data breach by $14. And In contrast, compliance failures can increase the cost by an average of $11.9.
- If the breach took place when the company was migrating an extensive amount of data to the cloud, the cost increased by $11.9 due to the complexity of determining the types of data lost or stolen.

Cyber safety tips:

- Train your employees to verify links, verify the sender and email address before opening an email or attachment. Employees should understand the dangers of visiting harmful websites, leaving their devices unattended and oversharing their information.
- Check up for your anti virus software: research to make sure you have the best for your business, Simulate an attack to see where the weakness is. Fix vulnerabilities and bugs.
- Strengthen passwords with numbers and symbols and change them every 6 months.
    - 9 characters can be figured out in 5 days
    - 10 characters in 4 months
    - 11 characters in 10 years
    - Note: the number of entries have increased from thousands per minute to millions per minute.
- Multi factor authentication- more than just a password other information that is needed to access the account
- Back up the data – protect from loss of critical data or proprietary data
- Create an incident response plan with cyber liability insurance and eliminate confusion by providing a step by step procedure to protect your customers, clients, employees and partners from financial and reputational damage.

If you have questions about how to protect your business from a cyber or breach threat, or have additional questions on any insurance questions please reach out to MarciaBrogan.com or 716.684.6000

Christopher Goss	Vice-President	Philadelphia Insurance
Marcia C. Brogan	Marcia C Brogan Agency	MarciaBrogan.com

A NYS, NYC, COUNTY OF ERIE, CITY OF BUFFALO
CERTIFIED WBE COMPANY
Phone: (716) 912-1803 | Toll-free: (800) 444-5530 | Fax: (716) 684-6285
marciabroganagency@gmail.com | MarciaBroganInsuranceAgency.com