What Every Business Should Know About Cyber Risk Management and Insurance

Lillian Romero-Gomez
President
Baker, Romero & Associates
Insurance Brokers, Inc.

"Providing insurance services to the community since 1986."

Disclaimer: For educational purposes only, not intended to be legal or insurance advice.

Cyber Crime Motivation

Most cyber criminals are motivated by greed. Cyber criminals primarily profit through fraud and extortion. Criminals are continually coming up with new and creative ways to illegally obtain data.

Cyber Attacks: Numbers and Statistics

- Cyber crime is the fastest growing form of criminal activity

- 44% of small business reported being the victim of a cyber attack

- The average cost of defending a cyber attack for businesses of all sizes is **$200,000**

60% of businesses go out of business within six months of being victimized

**https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Cyber Crime Stats 2020

1. Attacks on cloud services reached nearly 7.5 million in the second quarter
2. The detection of pandemic-related cyber attacks grew by **605%** in Q2 2020
3. On average, there are **419 new threats per minute**
4. Publicly disclosed security incidents increased by 22% in the second quarter including:
   - 35% malware attacks
   - 17% account hijacking, and
   - 9% targeted attack

~Figures from BusinessLine

Cyber Crime Concerns 2020

A recent study revealed the following as the top cyber concerns for Companies of all sizes (in order):

1. Employees unintentionally infecting the Company’s network with malware (responding to phishing e-mail, going to a bad website);
2. A cyber attack via malware;
3. Privacy violation/data breach of customer records;
4. Reputation damage due to privacy violation/ loss of customer records;
5. Employees unintentionally giving sensitive information to a 3rd party via social engineering;
6. Vulnerability in operations and/or outsourced to contractors (level of security at vendors and suppliers);
7. Theft/loss of organization’s assets/intellectual property due to a cyber attack;
8. Bring your own device or mobile security device use;
9. Fines and penalties in response to a cyber attack from government regulations

*Advisen, October 2020

What is Risk Management?

Risk Management prepares your organization for the unexpected. It deals with uncertainty and risk.

Good Risk Management is good management.

Risk Management Overview

- **Risk Management Basics**
- **BR Cyber Claims Reported During the Pandemic**
- **Cyber Risk Management Tips**
- **The Impact of COVID-19**
- **Cyber Risk Insurance**

Risk Management Basics

- Create/Organize/Update your risk management team to evaluate cyber security

- Identify risk and implement an action plan

- Evaluate risk

- Control risk *(Insurance)*

- Continuous Review

BR: Cyber Claims Reported During the Pandemic

- **Ransomware- A type of malware that attempts to deny access to a user’s data until a ransom is paid.**
  - *Client informed us that they received an e-mail indicating they could not have access to their data unless they paid $10,000.*

- **Phishing – A technique for attempting to acquire sensitive data, such as bank accounts, or access to a system through a fraudulent solicition in e-mail or on the website.**
  - *Client informed us that their accountant had recieved an e-mail from the “director” requesting a check for $2,500. The accountant paid the amount before discovering the scam.*

- **Stolen Laptop –**
  - *Client had laptop stolen from their vehicle. The laptop was personally owned by the employee and had confidential information (list of employees' social security numbers).*

Risk Management Controls: Back to Basics

- **Back up your computers** – Frequent backups of your system and other files
- **Store your backups separately** – Make sure your backups are stored on secure, separate devices that are not accessible from your network.
- **TRAIN your organization** – Raise cyber security awareness of employees and volunteers with regular training sessions. Remote workers are especially vulnerable and need to be continually updated on security measures and company policies.
- **UPDATE and PATCH your computer** – Ensure applications and operating systems have been updated with the latest patches.
- **Use caution with links and website addresses** – Be careful when clicking directly on links in e-mails, even if the sender appears to be someone you know.
- **Open e-mail attachments with caution** – Be wary of opening e-mail attachments, even from senders you know, particularly when attachments are compressed files or ZIP files.
- **Use and maintain preventative software programs** – Install antivirus software, firewalls, e-mail filters and keep them updated.

Risk Management: COVID-19 Impact

The defense against cyber events begins with education of the remote workforce and shared understanding of the challenges.

Safety Reminders for the Organization:

- Secure the network and applications from the organization side.
- Use VPN (Virtual Private Network)
- Regularly Update all systems and apply patches where recommend
- Secure virtual communications e.g., ZOOM, Skype, Google Chats, etc.
- Continually update your employment policies relating to use of technology, personal devices, etc.

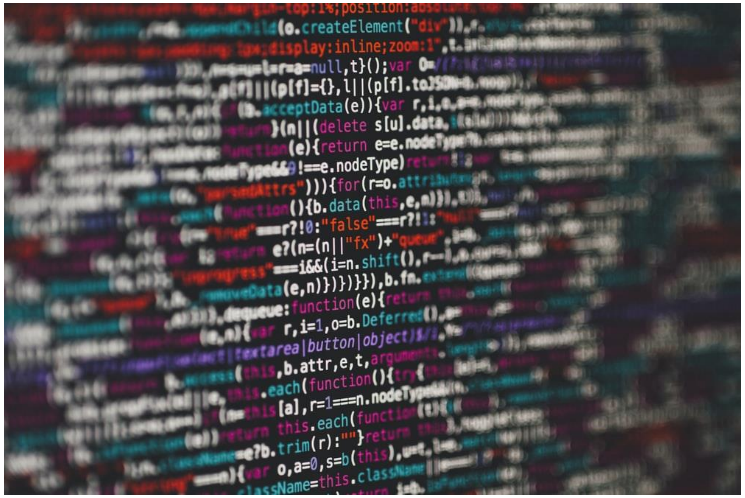
Safety Reminders for Remote Workstations:

- Don’t provide personal information including passwords.
- Use hard-to-guess passwords and change passwords frequently
- Never click attachments or links in e-mails without verifying their legitimacy with IT
- Change the default administrator password on all home routers and devices
- Ensure all personal devices are current with patches, and system updates
- NEVER store sensitive data on personal devices.

Risk Management: Cyber Insurance

A special form of insurance created to protect businesses against cyber (internet) risks, such as hackers and other breaches of computer system security.

Cyber Insurance plays a critical role in business. It allows a business to transfer cyber crime costs.



Risk Management: Cyber Coverage Options

Before you purchase a cyber policy, make sure you understand what your other insurance policies cover.

Many insurance carriers now offer a ***sublimit*** of cyber coverage. Coverages that may include some Cyber Loss Coverage may be found in the following:

- General Liability
- Business Package
- Crime
- Professional Liability
- Directors & Officers Liability
- Employment Practice Liability

Note: The cyber coverage under these policies is usually limited.

Risk Management: Cyber Insurance

1. There are over 55 active insurance companies in the marketplace offering stand alone cyber coverage. In other words, not combined with any other insurance coverages.

2. While there is a move toward standardization of coverage forms, there is no “standard” cyber policy. Every insurance carrier has their own coverage terms and conditions, which is why it is important for you to work with your broker to make sure that your policy fits your organizational needs.

3. Cyber Policies are written on a **claims made** form. Always check the **Retro Date** if you change insurance carriers**.**

4. Insuring Agreements: “Pay on behalf of” vs. Indemnity/Reimbursement.

5. Cyber policies may provide both first-party property and third-party cyber liability coverage.

6. Be aware of deductibles and sublimits of coverage.

7. Many Cyber insurance policies offer free or low-cost risk management service including notifications, working with counsel, etc.

Example Cyber Insurance Policy (stand alone)

- *Security and Privacy Liability (defense expense, damages, judgements, etc.)*
- *Website Publishing Liability*
- *Programming Errors or Omissions Liability*
- *Additional Insureds (as required by contract)*
- *Loss Expense Coverage:*
  - *Replacement or Restoration of Data*
  - *Extortion Costs*
  - *Business Income and Extra Expense sublimit*
  - *Cyber Crime Loss Sublimit (loss of $ from social engineering)*
  - *Public Relations Expense sublimit*
  - *Identity Monitoring sublimit*
  - *Security Breach Expense sublimit*

Types of Optional Cyber Risk Management Services:

- *Crisis Management Services*
- *Computer Forensics*
- *Crisis Public Relations*
- *Hot Line – legal assistance*

Cyber Risk- Insurance Underwriting Concerns:

1. What security measures does your organization have in place to protect your data, private customer and employee data from a breach? How often are security measures reviewed?

2. Do you have a crisis management plan? Crisis Management Team? Plan to deal with Regulatory Requirements?

3. Selection of Tech Providers: Do you thoroughly investigate your tech providers work history and experience? Do you always obtain certificates of insurance?

4. Are employees properly trained on how to update virus protection software and how to create hard to guess passwords?

5. Does your organization have HR and social media policies to reduce your risk and make sure all employees are trained?

6. Is there a formal program in place to evaluate the security posture of vendors?

NOTE: If your data is outsourced, remember that most cloud providers do not accept liability in their service agreement. Consult with your attorney for review of your agreements.

Additional Information

Website: Database for Breaches

History of All Data Breaches in U.S.

www.privacyrights.org/data-breach

Verizon Annual Data Breach Study

(this is the annual report most insurance underwriters review.)

www.verizonenterprise.com/DBIR/2020

Cyber Security Law: State of California

Caution- Breach Notification Requirements

In California, cyber security law is enforced by the Attorney General's Office. The State of California requires a business to notify any California resident whose unencrypted personal information, (e.g. birthdays, social security numbers, credit cards), was acquired, or reasonably believed to have been acquired, by an unauthorized person.

Aside from the reporting requirement, California requires a credit monitoring services for one year for those affected by a cyber breach. California law continues to evolve on this matter.

California has suffered more data breaches and has had more personal records exposed than any other state in the U.S. over the past decade.

*Comparitech Report: "Which State Has The Most Data Breaches?" https://www.comparitech.com/blog/vpn-privacy/data-breaches-by-state/

Final Thought…

“Good Risk Management fosters vigilance in times of calm and instills discipline in times of crisis.”

~ Dr. Michael Ong

Baker, Romero & Associates, Insurance Brokers Inc.

- Best “A” rated insurance carriers.
- Free H.R. Services through *H.R. Netline*
- Insurance and Benefit Review
- Loss Control Programs
- Financing Options
- No Broker Fees
- Free Educational E-Mail Blasts
- Educational Webinars and Seminars

THANK YOU!

Baker, Romero & Associates
Insurance Brokers, Inc.

750 Terrado Plaza, Suite 238, Covina, CA 91723

626 332 2258 (ph)
lillian@bakerromero.com
www.bakerromero.com

"Celebrating over 34 years of insurance service to the community."

DISCLAIMER: For educational purposes only, not intended as legal or insurance advice.