



WALSH

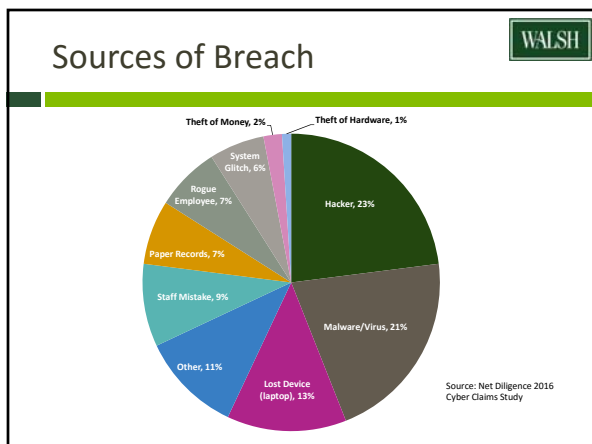
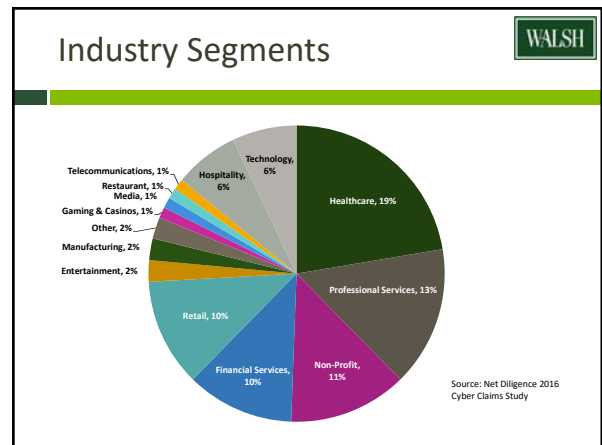
Privacy & Security Coverage

“Cyber insurance is a product used to protect businesses and individual users from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities.”

WALSH

What is Cyber Insurance?

- Deals with the breach of PII, PHI, or the valuable intangible property assets of you or your customers – trademarks, customer contracts, customer lists, employments contracts, to name a few
- Can provide the backstop to protect a business from the financial burden resulting from a breach
- Insurers are denying claims for cyber exposures under standard Property & Casualty coverage




WALSH

What does it look like?

- Majority of policies start with a focus on breaches, but most offer liability, remediation, regulatory fines and penalties, PCI fines and penalties.
- 69 companies in 2016 (\$3.35 billion) writing non-standard policies, tailored to the individual account
 - Terms can be negotiated
 - Policy limits/sub limits differ
 - Terminology is proprietary among carriers
- Most standard property and liability policies are not intended to provide coverage
- Carrier evaluations include:
 - Type of business
 - Revenue
 - Amount and type of data
 - How the business manages it people, process and technology

What does it look like? WALSH



Start with an assessment of your business to determine how a policy can protect you

- Coverage is being modified to meet the changing needs of customers, and underwriting is being refined to evaluate the emerging risks
- Product should be tailored based on exposures and risk assessment
- Know your options
 - Enhancements to existing policies (can be limited)
 - A stand-alone policy
- Obtain an indication for a premium range, and determine if it fits your risk management program.
Note: An actual application is required prior to binding.

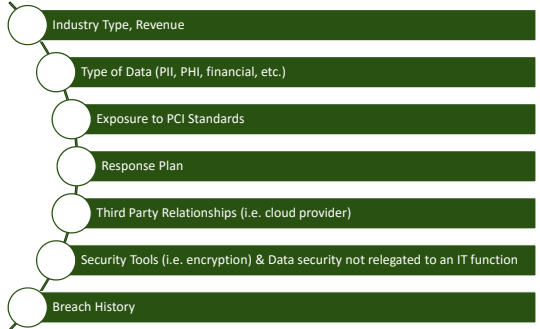
But, Do I Need It? WALSH

Remember: Every business utilizes technology

Know what is/isn't covered in General Liability or Property Liability policies

- We do not sell online (not just retail)
- We have the best IT security
- My business is not a target
- I don't collect or store data
- Do I need another policy? I cannot afford it.
- Shouldn't I invest in additional IT security/loss prevention?
- We use a third party

The Process WALSH



- Industry Type, Revenue
- Type of Data (PII, PHI, financial, etc.)
- Exposure to PCI Standards
- Response Plan
- Third Party Relationships (i.e. cloud provider)
- Security Tools (i.e. encryption) & Data security not relegated to an IT function
- Breach History

Issues/Exclusions in Policies WALSH

- General Liability – ISO exclusion as of June 2014
 - GL policy does not cover data privacy breach losses
- D&O/E&O/Property/Crime
 - Maybe partial coverage
- Sublimits or enhancements to your policies
 - BOP, but not a catchall

What do you need in a policy? WALSH

- Notification costs in the event of a breach
- Credit monitoring
- Forensics to identify the source of the breach and repair it
- Legal costs incurred
- Public relations for reputational damage
- Fines and penalties imposed by regulators or the PCI industry
- Business interruption – loss of income
- Extortion threats
- Cyber terrorism
- Lawsuit resulting from a data breach, denial of service or other damage

A Close Look at Building Cyber Coverage WALSH

- Customization and non-standard forms
- Definitions and exclusions
- Conditions, limits, warranties
- Prior acts
- Claims made
- Selection of counsel or carrier may reserve the right to select or at least approve counsel. Negotiate agreement on choice of counsel.
- Risk Management services
- Failure to maintain security standards*
- Endorsements to add coverage
- Notice of Loss
- Limited fines and penalties

Risk Management is Key WALSH

- Have you raised the level of cyber awareness within your organization?
- Do you have a designated person who is responsible, and is management accountable?
- Are employees educated on cyber exposures?
- Do you conduct regular training?

Risk Management is Key WALSH

- Do you have an encryption policy?
- Do you have a written privacy policy?
- Are your formal written policies and procedures reviewed?

Risk Management is Key WALSH

- Do you segregate and protect personal identifiable information?
- Do you know the amount of private information or records you have?
Realize the size and scope of threats through an assessment
- Do you update your intrusion detection software, data backup, build-in redundancy?
- Have you reviewed your contractual obligations?
- Are you compliant with industry standards and privacy laws?

In Summary WALSH

- Complacency is not the posture, you need resilience
- Evaluate risk through an assessment
- Mitigate risk through IT solutions
- Have an action plan in the event of a breach
- Consider risk transfer – contractual, avoidance, insurance

Become cyber resilient!

Questions? WALSH

Carol A. Wageman, CIC
Vice President – Walsh Duffield Companies, Inc.
716.362.7328
cawagemen@walshins.com



Cyber Security Breach Claims Examples

Remember - Any business that has access to confidential personal information faces the threat of a data breach, regardless of size or industry.

Scenario: Stolen laptop

A physician suffered a burglary at his residence and his work laptop was stolen. The laptop had his entire 15 doctor medical group's patient database on it comprising 37,000 unique identities. The medical group was required to publish a notice of the breach on their website and in the local media. Additionally, the group was required to notify the Office of Civil Rights of the breach, which led to a Department of Health and Human Services investigation, and a required HIPPA compliance review. The total expense for this breach was \$44,000.

Scenario: Hackers

A physician office's server, which contained unencrypted protected health information (PHI) for 2,500 patients, was accessed by hackers and encrypted. The hackers subsequently made an extortion demand of \$50,000 to decrypt the information and return control of the server back to the physician's office. After retaining a negotiator at a cost of \$45,000 and complying with the hackers' financial demand, control of the server was returned to the physician's office. Thereafter, the practice incurred \$85,000 in expenses associated with notifying patients regarding the event, hiring a public relations firm, establishing a call center, providing monitoring services, and retaining independent counsel to assess notice and compliance obligations. A subsequent audit from the Office of Civil Rights resulted in a \$75,000 fine to the practice under the Health Information Technology for Economic and Clinical Health (HITECH) Act for not having encrypted the PHI.

Scenario: Skimming Devices

A criminal syndicate attached skimming devices to a local retail chain's payment card systems at a variety of locations. This permitted unauthorized access to the credit and debit card information of 15,000 customers over a three-year period. The retail chain spent \$850,000 performing forensics, engaging counsel for compliance assessment and providing notification and call center services to its customers. It also spent \$900,000 reimbursing a variety of banks for costs associated with card cancellations and re-issuance charges. Lastly, it spent \$75,000 in defense costs responding to a regulatory inquiry and \$250,000 in fines.

Scenario: Invasion of Privacy

A manufacturer leased a copy machine over a two-year period. During that time, the company made copies of proprietary client and employee information, including social security and driver's license numbers. After the lease expired, and prior to making its way back to the leasing company, a rogue employee accessed the machine's data for nefarious purposes. The manufacturer incurred \$75,000 in expenses in connection with a forensic investigation, notification, identity monitoring, restoration services and independent counsel fees. It also incurred approximately \$100,000 in legal defense costs and \$275,000 in indemnity associated with the theft and sale of proprietary client information.



For more information, contact:

Carol A. Wageman, CIC
Vice President
Walsh Duffield Companies, Inc.
cawageman@walshins.com
716.362.7328

Know what to look for in your cyber insurance coverage. While policies are non-standard, these are the general risks cyber insurance covers:

Breach Response Costs

- Notification Costs and credit monitoring; perhaps a call center
- Breach coach/legal services to guide you through the breach
- Public relations – minimize reputational harm – usually a sublimit to restore your corporate reputation
- Forensics – identify the source of the breach, magnitude and how to fix it
- Repair – fix the weakness in the system

Liability Insurance

- Legal costs and settlements for a lawsuit that alleges a failure to protect confidential information

Fines and Penalties

- Imposed by regulators
- Imposed by credit card processors

Extortion

- To cover the cost of ransom-type payments to cyber criminals that threaten to corrupt data, shut down a website

Theft

- Of the economic value of funds, goods or services

Business Interruption/Extra Expense

- Loss of income arising out of the inability to operate
- Extra Expense to continue or resume operations more quickly

Social Engineering Coverage

- Theft losses from deceptive funds transfer

Return this form to:

Walsh Duffield c/o Grace Brightman

gbrightman@walshins.com

801 Main Street

Buffalo, NY 14203



Walsh Duffield
Insurance since 1860

SIMPLIFIED PRIVACY / SECURITY APPLICATION

This will allow us only to get an indication of pricing. Full application is needed to secure bindable terms

Insured:

Street:

City: / **State:** / **Zip:**

Nature of Operations:

Average number of active / inactive records? (Employee, Client, Credit Cards, Medical records etc.)

Annual revenues?

Type of records maintained?

What types of activities does the insured perform on the internet?

Are the Insured's services business to business or business to customer?

Does the Insured have procedures in place to comply with privacy regulations?

Does the insured collect; receive; transmit; or store confidential information. i.e. social security numbers; bank numbers; credit card numbers, etc?

Is the insured's website hosted by a third party?

Does the insured or a third party perform penetration testing on their firewalls?

What type of security procedures are in place?

Phone: 800-853-3820

www.walshins.com

Fax: 716-847-1360