{ Holmes Murphy & Associates }

We're for you.

Cyber Security Liability: Best Practices

Nick Maletta, Cyber Liability Practice Leader

HOLMES MURPHY®

Top 5

1. Identify what you have
2. Breach Incident Response Plan
3. Educate Employees
4. Keep up to date, implement some level of Security
5. Protect your Balance Sheet with Insurance

Identify Exposure

- HMA Self Assessment
  - Holmesmurphy.com/infosecurity
- Symantec Assessment
  - https://databreachcalculator.com/
- Number of Files, number of employees
- Really need to quantify the potential and have an idea of what is at risk
- Don't: Think you're not a target

Incident Response Plan

Create a breach response plan

- Know what types of data are stored and where
- Develop an ongoing plan to assess / monitor / evaluate privacy risk
- Create an ongoing compliance, education, and mitigation plan
- Develop a response plan for when a data event occurs (it will)

Typical components of a response plan for a data breach:

- Key members of decision team (C-suite and senior IT)
- Align vendors (Attorneys, PR, Forensic Security, Breach Response)
- Stop the breach
- Determine scope of breach (types of data, how much, who affected)
- Internal remediation – Forensic expertise/repair upgrades
- External party notifications (patients, State AG's, credit bureaus, police, FBI)
- Affected patient disclosure (meet state requirements, timing, scope)
- Notification (message, medium)
- External remediation (credit monitoring or other services)
- TEMPLATES ARE AVAILABLE!
- Don't: Become complacent

Educate Employees

- Weakest link
- Email protocols, password protection, phishing attacks, phone hacking, social engineering, traveling
  - Norse-corp.com; Haveibeenpwned.com; howsecureismypassword.net; echosec.net; spooftel.com; ComputerCrimeInfo.com
- Don't: Assume your employees know the right thing to do

Implement Security

- Cyber Hygiene
- Keep the doors to information closed when you can
- Inexpensive/Free guidelines or services you can implement
  - http://www.nist.gov/cyberframework/
  - www.holmesmurphy.com
- Don't: Assume a third party has got it taken care of

Cyber Hygiene

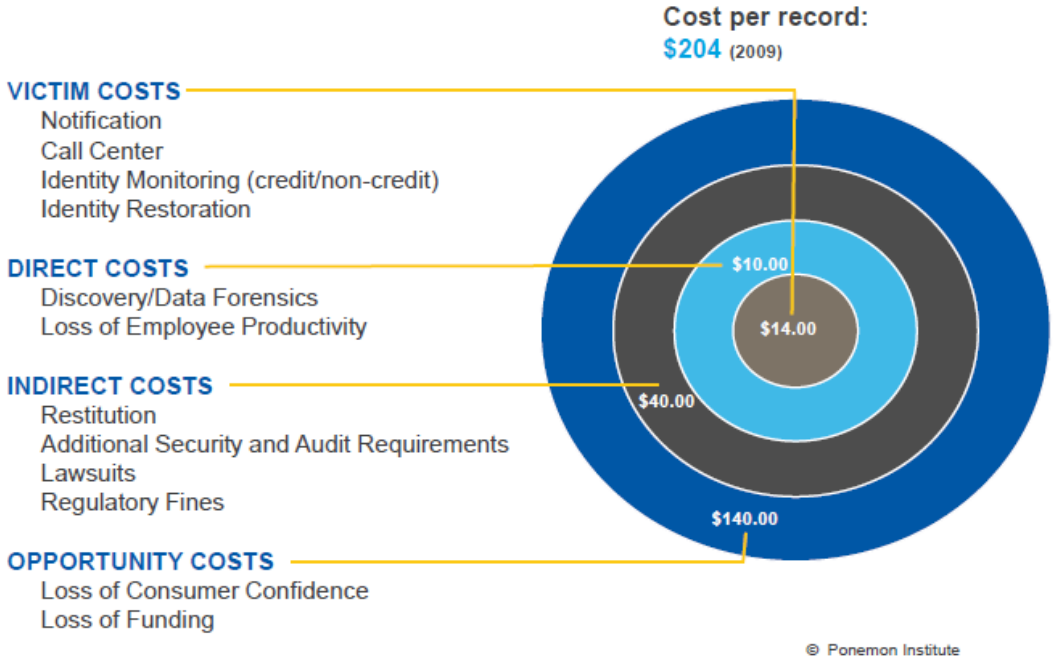
- Boring things
- Regularly updating software
- Routine audits of your systems
- Routine audits of your vendors
- Reviewing internal procedures and policies
- Keep online doors closed (laptops, smartphones, tablets, TV's)

Insurance Marketplace- Don't: Assume you can handle it all.

REACTIVE RESPONSE

Breach Costs

Breaches: By the numbers….
Cost of a breach record



The Coverage Gap

Unless specifically addressed, Privacy and Network Security Liability falls between the cracks of coverage provided by traditional insurance policies:

- General Liability – (may provide limited coverage) for "*publication of material that invades a person's right to privacy*"
- Commercial Property – electronic data extension only covers replacement of destroyed or corrupted data. Indirect or consequential loss excluded
- Commercial Crime / Computer Crime – generally excludes loss from theft of confidential information & excludes indirect or consequential loss
- D&O Policy – D&Os unlikely to be named. Some policies have invasion of privacy excluded in BI/PD or Personal Injury Exclusion. No 1st party expense coverage
- E&O Policy – generally respond only to loss from a defined professional service and typically no "first party" coverage for breach-related expenses

Carrier Selection

- Financial stability
- Coverage terms and conditions
- Appetite for clients in your industry
- Appetite for the size of your client's business
- Commitment to the product
- Claims paying reputation and infrastructure
- Industry expertise
- Relationships with expertise – attorneys, security firms, forensic specialists

Limits?

- Exposure for data loss is tied to the number of individuals you have information on
- Types of protected information stored
- Location and segregation of sensitive data
- Industry specific considerations
- How much do my peers buy?

Insurance Carrier Underwriting

Data/Confidential Info – Types/How much?/location

Encryption (Safe harbor) – At rest, in motion, backup, mobile devices

Systems & Software – Patches/updates/controls

Use of cloud vendors – who/what services (payroll, payments, services, etc.)

Vendor Controls – Due Diligence/ Contracts/Data shared/Access control

Network Access – How and who accesses your network remotely?

Subsidiary acquisitions – Due diligence, conversion process

Compensating controls – What else are you doing?

Coverage Considerations

- Exposure based concerns:
  - Corporate Confidential Information
  - Rogue Employee Coverage
  - Paper Records
- Exclusions to be mindful of:
  - ‘Not on Network’ devices, Known-virus exclusion, failure to maintain updates
- Vendor Agreements- Indemnity Flow
- Breach Estimator Tool:
  - https://databreachcalculator.com/

Cyber/Privacy Best Practices

Contracts – Cloud providers and Data Holders

- Review Vendor Agreements – Insurance Requirements, Indemnify
- Limitations of Liability / Indemnifications

Privacy controls/procedures

- Access to electronic information only as needed for employees
- Information is encrypted whenever possible
- Review of physical security procedures used at various locations
- Privacy policy in place, monitored for compliance, updated
- Sharing of customer information with any 3rd parties
- International privacy rules for data transfers

Claims, legal matters, and insurance

- Broker Interaction – Let them help with the process
- Provide leverage and discussion about coverage intent with carrier
- Work with coverage and outside counsel as necessary

Studies

- Verizon Compliance Study
- Ponemon Institute Study
- NetDilligence Security Report
- Symantec Corp.

- COMPUTERCRIMEINFO.COM

Questions?

Nick Maletta, Account Executive & Cyber Liability, Holmes Murphy & Associates

Nmaletta@holmesmurphy.com

(515) 223-6919

Self Assessment Survey

www.holmesmurphy.com/infosecurity