{ Holmes Murphy & Associates }

*We're for you.*

# The Wild West of Cyber Liability

Nick Maletta, Cyber Liability Practice Leader

HOLMES MURPHY

# NORSE-CORP.COM

# Current Events

- Community Health Systems
- SuperValu Grocery
- Albertson's
- McDonald's
- UPS
- JPMorgan
- Kleiner Perkins
- Healthcare.gov????
- Home Depot!
- Target
- Staple's
- WellPoint
- Apple
- Lenovo- Superfish
- Uber
- Anthem
- Forbes
- Dating Applications
- Dutch Government
- Sony
- Malaysia Airlines
- SnapChat
- Jimmy John's
- Dairy Queen
- K-Mart
- Eastern Iowa Airport
- HSBC
- Premera

# PROACTIVE APPROACH

# How to begin?

## 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)

# Employee Gap

- Weakest Link
- Technology can only do so much
- Education is Key
  - On everything from technology protocols to what not to leave on your desk at night
- Quick Tip- Traveling
  - Hotel Lobby Business Centers
  - 'Yahoo' Trick- http://mail.yahoo.com

# Employee Emails

- Phishing
- Vast majority of attacks are successful because employees click on tainted links in emails
- Roughly 2/3 of all 2014 attacks involved phishing
- 10 emails to employees produces roughly a 90% hit ratio
- If you are not sure, do not open, pick up the phone!
- Email Hacked?
  - https://haveibeenpwned.com/

# Social Phishing

- Social Phishing
  - https://www.echosec.net/
- Generate answers to your password security questions
- Can be done over the phone

# Password Protocols

- Password protection
  - A quarter of all breaches could have been stopped if more than just a password were required to enter a network.
  - KeePass
  - Security Questions
- Use different passwords for different websites – social media vs. banking
- Most common password= password (???)
- Strength of Password?
  - https://howsecureismypassword.net/

# 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)

# New Attacks

- Phone attacks- Spooftel.net
  - Because spotlight is on computer hacking, criminals are going "old school"
  - Getting phone numbers of Facebook and placing calls to loved ones claiming to care for family member
- RansonWare- hackers encrypt your files and promise to release them if the user pays a ransom.
  - 80% of the time they do not decrypt the files

# 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.

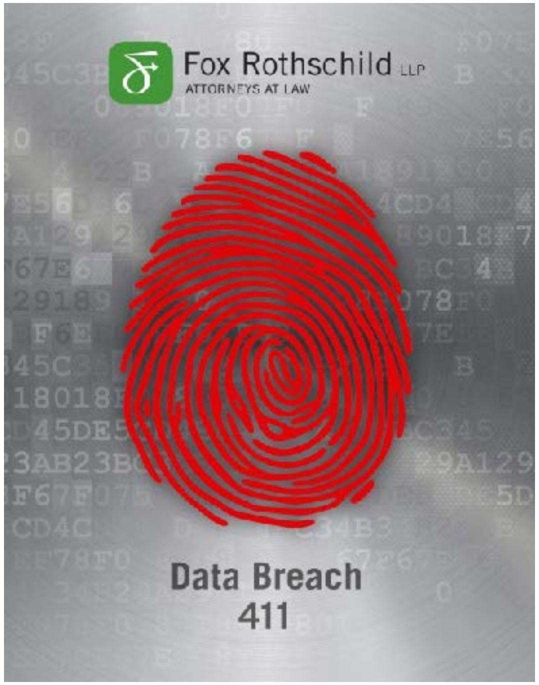
- COMPUTERCRIMEINFO.COM

HOLMES MURPHY

# EVOLVING LEGAL LANDSCAPE

# State Notification Laws

- 47 States have enacted Notification laws (As of July 15, excluding Alabama, New Mexico, South Dakota)
- Including DC, Guam, Puerto Rico, and Virgin Islands




# Iowa Law

- Iowa Code S. 715C.1, 715C.2
- Modified July 1, 2014- SF 2259
- Personal Information=First name or initial and last name in combo with...social security number, driver's license number, finance account info, unique electronic identifier, unique biometric data.  Not including publicly available info.
- New Amendment=Requirement to notify Attorney General or regulator in addition to notifying affected individuals where the breach affects 500 or more Iowa residents within 5 days of the breach.

# New Legislation

- April 23, 2015- National Cybersecurity Protection Advancement Act of 2015
- House passes 2nd threat-sharing cyber security bill (355-63)
- Extends liability protection for companies that share information about cyber attacks if data is given to the US Department of Homeland Security
- Still needs Senate and Executive approval
- Opposition- could lead to more surveillance

- Sanction program launched by the Obama Administration- April 1, 2015

# Federal Jurisdiction?

- HIPAA
- HITECH Act
- FTC Juridiction?
- NIST Plan
- PCI Compliance?

Insurance Marketplace

# REACTIVE RESPONSE

# 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

# Breach Costs

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

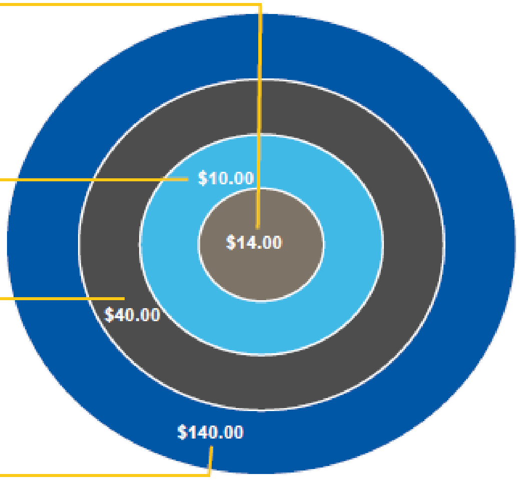
Cost per record:
$204 (2009)

**VICTIM COSTS**
- Notification
- Call Center
- Identity Monitoring (credit/non-credit)
- Identity Restoration

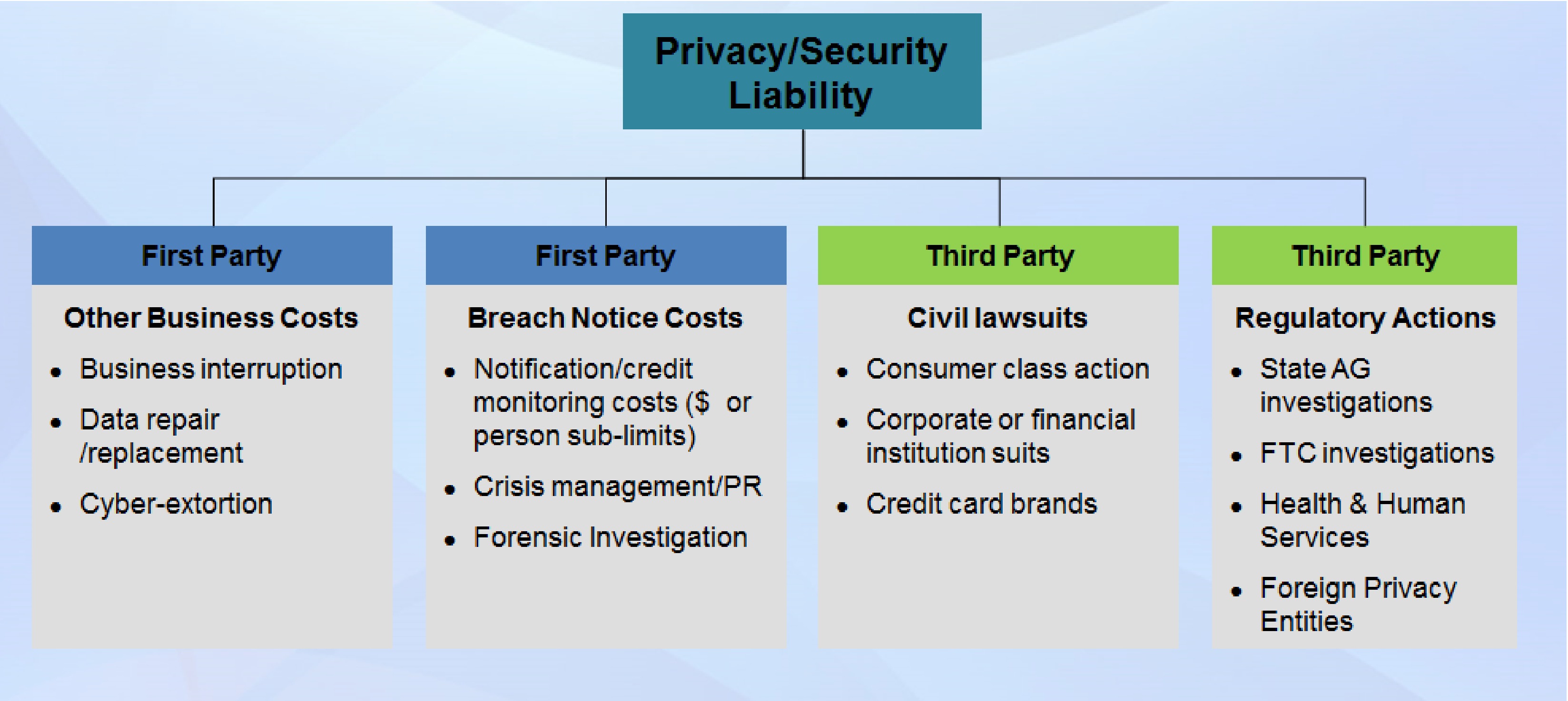
**DIRECT COSTS**
- Discovery/Data Forensics
- Loss of Employee Productivity

**INDIRECT COSTS**
- Restitution
- Additional Security and Audit Requirements
- Lawsuits
- Regulatory Fines

**OPPORTUNITY COSTS**
- Loss of Consumer Confidence
- Loss of Funding



# Coverage Structure



# Marketplace

# 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/

# Capability


BreachCommunications
SecurityBestPractices
RiskExposureReview
Compliance
FiduciaryLiability
ClaimAdvocacy
LossForecasting
UnderwritingInformation
ShareGroupForums
AuditTips
CoverageReview
ContractReview
SecuritySelf-Assessment
Benchmarking
InsuranceBuyingPower
PolicyAudits
ServicePlans
EmployeeBenefits
LossControl
DataBreachMitigation
DocumentedContinuity
InformationTechnologyConsulting
BusinessIncome

# Questions?

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

Nmaletta@holmesmurphy.com

(515) 223-6919

Self Assessment Survey

www.holmesmurphy.com/infosecurity

HOLMES MURPHY