HYLANT

Why Cyber Insurance Should be in Your Risk Management Toolbox

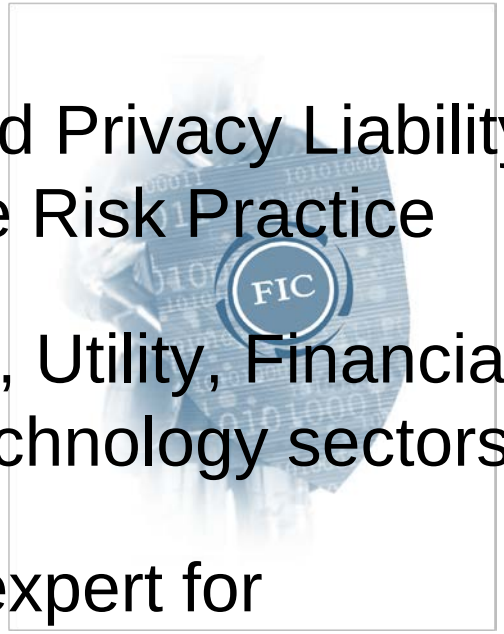
University of Dayton School of Law

June 3, 2016

Spencer Timmel, CIPP/US, CIPM, CITRMS
Scot Ganow, Esq., CIPP/US

HYLANT

Spencer Timmel, CIPP/US, CIPM, CITRMS



- Cyber Security and Privacy Liability Product Leader, Hylant's Executive Risk Practice
- Retail, Healthcare, Utility, Financial, Municipality, Education and Technology sectors.
- Cyber insurance expert for
  - CIAB (Counsel of Insurance Agents & Brokers)
  - Acord's Professional & Specialty Lines Working Group

Scot Ganow, Esq., CIPP/US

- Privacy and Security Law
  - Information privacy compliance
  - Data security and breach coach
  - Risk assessment, audits, policy development
  - HIPAA, GLBA, FCRA, PCI-DSS, COPPA
- 13+ years data privacy & compliance experience
- Certified Information Privacy Professional (CIPP)
- Former Corporate Privacy & Ethics Officer
- Adjunct Professor of Law, Univ. of Dayton

FIC

2015 PILT: Data Governance: So What's Your Story??

Spoiler Alert: It's not IF, but WHEN

Data Governance is your Story.

A. Information: What, Where, How and Who Uses It

B. Safeguards

1. Administrative
2. Technical
3. Physical

C. Accountability & Management (It never ends)

Get Covered: A Good Story Helps

A. Consider insurance to offset the impact of data breach.

   i. Liabilities

   ii. Litigation

   iii. Regulator inquiries

B. Consider additional services provided in some policies

   i. Breach coaches

   ii. Think of opportunity costs and time spent on breach and not your business

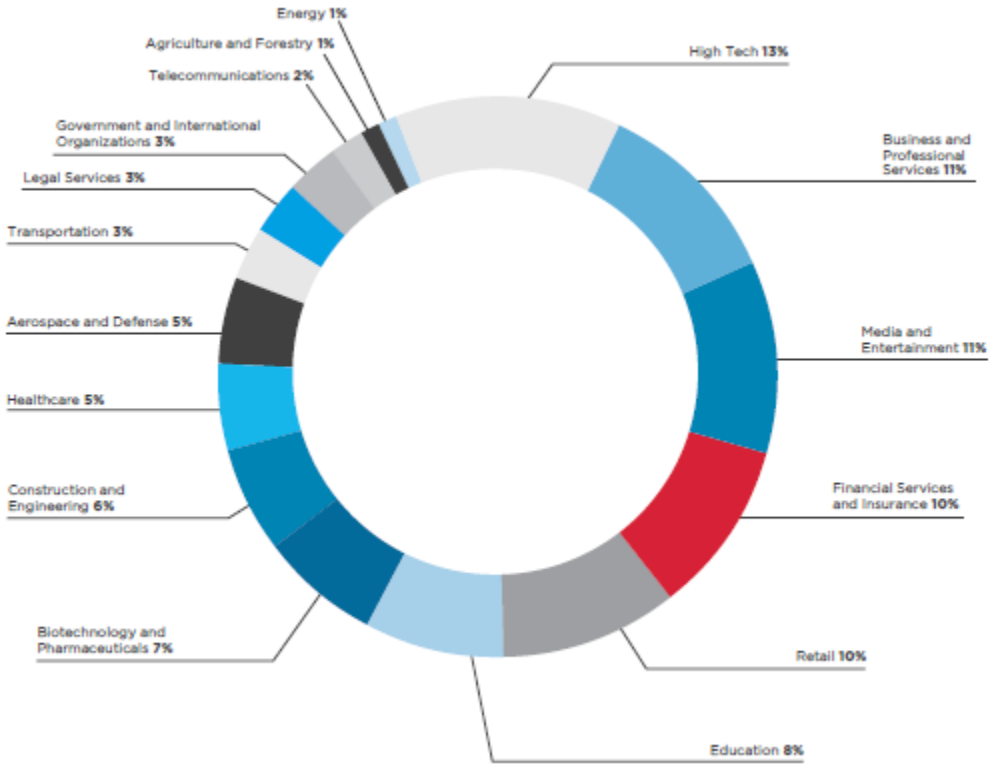
   iii. Breach response can be a marathon, not a sprint.

Cyber Liability Deeper Dive

- Threat Landscape
- Cyber Related Risks
- Data Privacy Costs
- Why has Cyber Insurance become so attractive?
- Marketplace
- Coverage
- Cyber Risk Evaluation: A Process
- Misconceptions
- Best Practices
- Group Exercise

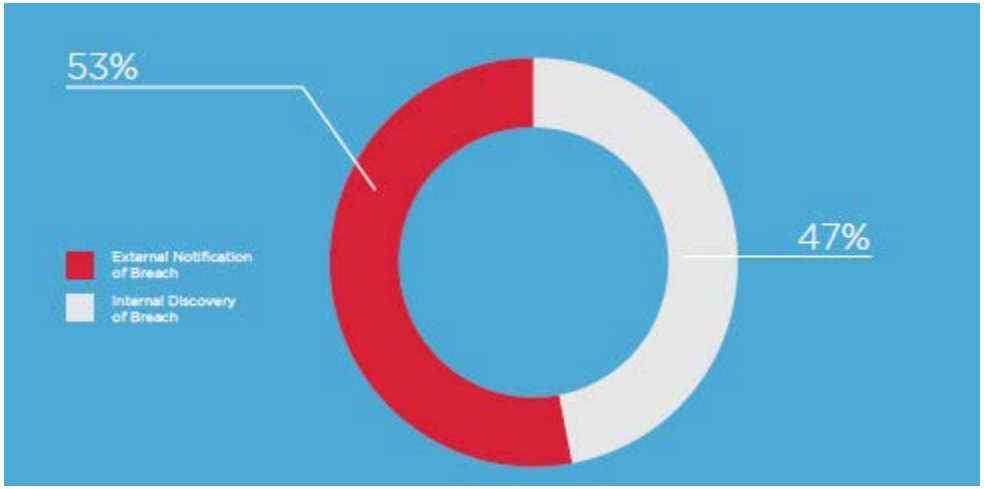
Cyber Risk Threat Landscape (M-Trends 2016)

- More INCIDENTS (not breaches) became public than at any other time in the past
- Locations and motives of the attackers were more diverse
- Industries Target: Anyone and Everyone



Cyber Risk Threat Landscape (M-Trends 2016)

- How are compromises being detected? (Internal vs External)



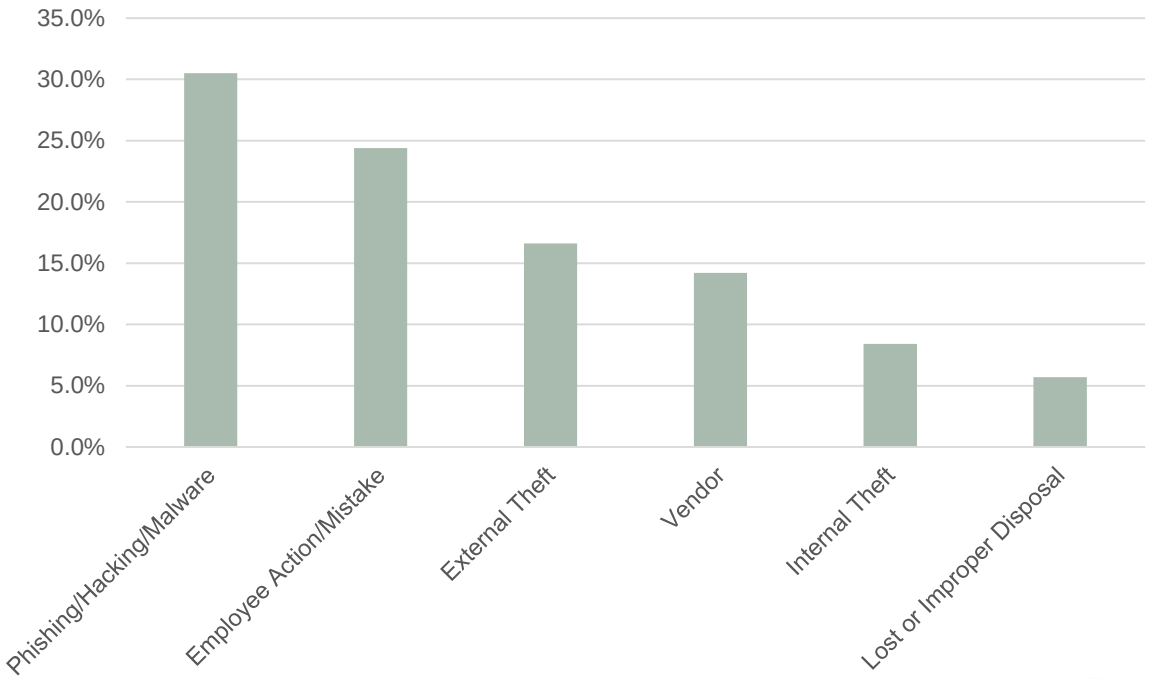
- Median Time it takes for an compromise to be discovery?

All Mandiant Investigations in 2015	External Notification	Internal Discovery
146 days	320 days	56 days

- Average Days to hacker gains Administrator Credentials? **3**

Additional Statistics

- 70% of organizations report having been compromised by a successful cyber attack in the past 12 months
- Security Incidents grew 66% year over year
- Data Privacy Cause Statistics



Cyber Security and Data Privacy Risks

- Data Privacy:
  - Improper Disclosure of Information: PII, PHI, PCI
  - Improper Collection of Information: COPPA
  - Improper Contact of Individuals: CAN-SPAM, Song Beverly
- Business Interruption and Extra Expense: eCommerce: Malware
- Reputational Injury: Target
- Asset Damage and Data Restoration: Saudi Oil company: Aramco- 30,000 PCs
- Bodily Injury and Property Damage from Nonphysical Triggers:
  - control systems for heart rate monitors, traffic lights, home security apps, cars-- many of which have no security protocols of any kind built in.
- Extortion: Armada Collaborative-DDoS Threat
- Social Engineering Crime Claims: “wilful transfer of funds”

Data Privacy Costs?

Breach expenses	Liability	Regulatory	Reputational Injury
			
Notification	Damages to affected parties	Regulatory Defense	Lost Customers
Credit monitoring	Legal defense costs	Fines and penalties, incl. PCI	Canceled Contacts
Forensics			
Legal guidance			
Crisis communication			

Cost of a Data Breach?

- Ponemon Study
  - $217 per record; $6.5 million
  - 35% is direct costs; indirect costs-loss of customers and reputational injury
  - 100,000 records or less

- NetDiligence Claims Study
  - Estimates only 5% of the total number of claims handled by all markets
  - Represents Claims payouts not costs to the insured: policy construction/broking/sublimits
  - Median cost per record: $13
  - https://eriskhub.com/files/articles/NetDiligence_2015_Cyber_Claims_Study_eRiskHub_Expanded_Edition_093015.pdf

Cost of a Data Breach?

- Verizon Data Breach Report
  - All forms of data

RECORDS	PREDICTION (LOWER)	AVERAGE (LOWER)	EXPECTED	AVERAGE (UPPER)	PREDICTION (UPPER)
100	$1,170	$18,120	$25,450	$35,730	$555,660
1,000	$3,110	$52,260	$67,480	$87,140	$1,461,730
10,000	$8,280	$143,360	$178,960	$223,400	$3,866,400
100,000	$21,900	$366,500	$474,600	$614,600	$10,283,200
1,000,000	$57,600	$892,400	$1,258,670	$1,775,350	$27,500,090
10,000,000	$150,700	$2,125,900	$3,338,020	$5,241,300	$73,943,950
100,000,000	$392,000	$5,016,200	$8,852,540	$15,622,700	$199,895,100

Risk Transfer: Why has the insurance become so attractive?

- Inability to completely eliminate all risks through…
  - IT security Investments
  - Indemnification Provisions with 3rd party vendors
- Board Level Pressures
- Regulatory Efforts, Increased Legislation, and Ever Creative Plaintiffs Bar
- Alignment with Breach Response Teams
- Proven Balance Sheet Protection…PAID CLAIMS

What does the marketplace look like?

- 50+ insurance companies, including Lloyds of London: Continued race for market share
- Global Capacity- 3rd Party Liability: $350M; 1st Party Business Interruption: $250 Million
- Lack of IT security knowledge — especially insurance agents: placement and claims advocacy
- Buyers Market: Premium; Deductibles; Manuscript Language
- Varying appetites based on industry and size

Employment Practices	Private / NP D&O	Cyber 2015	Cyber 2020	Cyber 2025
$1.7 Billion	$2 Billion	$3 Billion	$10 Billion	$20 Billion

Insurability – 3rd Party Coverage

Privacy Breach Expenses/Crisis Management Expenses:

- Notification Costs
- Credit Monitoring
- Forensics
- Crisis Communication
- Breach Coach; Legal Guidance; Attorneys fees to determine actions necessary to comply with state laws

Privacy Liability Defense and Indemnity

- Class Actions from Affected Parties

Regulatory Defense & Fines/Penalties (if insurable)

- State AGs, FTC, Office of Civil Rights, HHS, International Regulators
- Regulatory Fines and Penalties, including PCI Assessments

Electronic Media Liability/ Internet Liability/Content Liability

- Invasion of privacy, plagiarism, libel, slander

Insurability – 1st Party Coverage

Business Interruption/Extra Expense

Reputational Injury

Data Restoration/Digital Asset Coverage

Cyber Extortion

eTheft and Social Engineering: Willful Transfer of Funds

Nonphysical Trigger for Property Damage and Bodily Injury

Cyber Risk Evaluation: A Process

- Inventory the Data
    - What type of data? PII;PHI;PCI
    - How is it stored?
    - How long is it at risk?
    - How many potentially impacted individuals in a Catastrophic Incident?

- Identify the Risk
    - 4 Buckets of Data Privacy Costs
    - Other Cyber Risks
        - Improper Collection
        - Improper Contact
        - Business Interruption and Extra Expense
        - Computer Asset Damage and Data Restoration
        - Bodily Injury and Property Damage
        - Social Engineered Crime Claims
        - Extortion

Cyber Risk Evaluation: A Process (cont.)

- Quantification of Risk: Catastrophic Modeling vs Average Cost
    - Use multiple sources
    - Understand Benchmarking Limitations
    - Business Interruption Worksheets?

- Mitigate the Risk
    - Understand Indemnification Limitations with Vendors
    - Become Compromise Ready

- Transfer the Risk: Insurance
    - Don’t assume quoted terms correspond directly with your risks
    - Always question sublimits
        - Regulatory Defense & Penalties
        - Forensics
        - PCI Assessments
    - Never accept mobile device or maintenance exclusion
    - Tell your own story
    - Consider Alternative Risk Transfer Strategies

Misconceptions

- “I’m not a target”
- “Insurance doesn’t pay”
- “Insurance can’t fit my real need”
- “I want to get my ducks in a row first”
- “Underwriters don’t care about our real story”

Check List

- Are there sublimits under my program?
  - PCI Fines/Penalties/Assessments
  - Regulatory Defense, Fines and Penalties
  - Forensics
- “What do the stand alone exclusions mean to my specific exposures?”
- “Does Regulatory coverage trigger on investigation or proceeding?
- “Is the policy form enhanced every year?”
- “Is the broker pushing market competition at least every other year?”
- “Is there confirmation the vendors that are part of my incident response plan have been approved and written into the contract language?”

Client Best Practices

1. Regularly Inventory Data:

   What kind? How Much? Where is it? Who has access? How is it protected?

   Health Data? Log-In Credentials? Credit Cards Data? Financial Data? SS#?

2. Evaluate contracts with outside service providers, specifically 3rd party IT, data storage or data processing vendors

3. Require and obtain certificates of insurance for both Professional E&O and Privacy/Cyber Liability coverage

4. Regular 3rd party security assessments

5. Updated incident response team with experienced outside vendors:
   "Align with Insurance Coverage"

6. Test the incident response plan with table top exercises

7. Insurance as a "Safety Net" to other internal and external safeguards

Spencer Timmel, CIPP/US, CIPM, CITRMS |
Hylant
513-354-1656
spencer.timmel@hylant.com

Scot Ganow, Esq. CIPP/US
Faruki Ireland & Cox P.L.L.
937-227-3716
sganow@ficlaw.com