INSURANCE CONSIDERATIONS FOR PRIVACY RISKS

A CONTINUING EDUCATION COURSE

CYBERSECURITY RISK AND CYBER INSURANCE ARE…

1

RICHARD S. PITTS

Vice President and General Counsel
ARLINGTON/ROE & CO., INC.

Executive Vice President
MUTUAL INSURANCE COMPANIES ASSOC. OF INDIANA

8900 Keystone Crossing, Suite 800

Indianapolis, Indiana 46240

2

CYBERSECURITY RISK AND INSURANCE ARE…

1. The Risk is Overwhelming
2. …But the Principles Are Conceptually Consistent
3. The Legal Landscape is a Swamp of Litigation and Regulatory Developments
4. …But it all remains an Insurable Exposure (but with some Caveats)

3

CYBERSECURITY RISK IS OVERWHELMING

SECTION ONE

4

INSURANCE BUSINESS AMERICA (7/6/19)

- 57% of Americans are very worried about cybersecurity issues
- 53% are concerned about online payments and purchases
- 42% fear identity theft
- 48% think companies aren't doing enough to protect their information

5

INSURANCE BUSINESS AMERICA (7/6/19)

"[Hiscox reported] 61% of firms suffered a cyber attack in the past year, compared to 41% the year prior. The median cost for losses associated with cyber incidents shot up from $229,000 to $369,000."

6

INSURANCE BUSINESS AMERICA (7/6/19)

- 72% of the American companies surveyed plan on spending more money in the next year on cyber than they did the year past.
- However, only 11% were going to put more money into training and cultural changes resulting from an incident.

7

THE PROBLEM IS PARTICULARLY ACUTE FOR SMALL BUSINESSES

Hiscox reports

- 52% of small business don't have a strategy
- 46% of small businesses have a defined role for a leader involving cyber
- Almost 2 in 3 small businesses have failed to take action following a cyber security incident.
- Less than a third of businesses have "phished" to assess behavior and readiness

8

CYBERSECURITY IN 2021 - MIMECAST

- With employees around the world trading cubes, offices and conference rooms for email, instant messaging and Zoom meetings, more sharing of sensitive business information has migrated from conference room white boards and face to-face conversations to discussions via collaboration tools and extended email threads. This swell of digital activity has presented cybercriminals with numerous new openings for social engineering attacks.
- *To wit, during 2020, the Mimecast Threat Center detected a 64% rise in threat volume compared to 2019.*

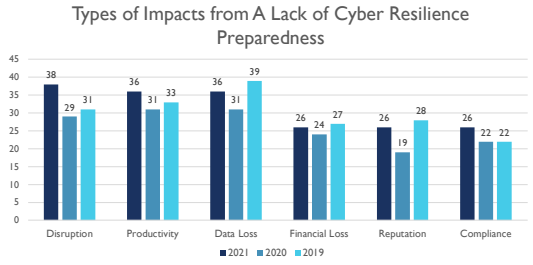
9

CYBERSECURITY IN 2021 - MIMECAST

79% of the [State of Email Security (SOES) survey] respondents acknowledge that their company experienced a business disruption, a financial loss or some other setback due to a lack of cyber preparedness. Unsurprisingly, given the intensity of the post-COVID threat climate, this was significantly higher than in prior years.

10

CYBERSECURITY IN 2021 - MIMECAST



11

CYBERSECURITY LAW IS CONCEPTUALLY CONSISTENT

SECTION TWO

12

MULTIPLE LEGAL SOURCES

"There is no single law in the United States that provides a comprehensive treatment of data protection or privacy issues…In contrast to U.S. privacy law, privacy protection in Europe is addressed by omnibus legislation covering both public and private sectors."

Stratford and Stratford, "Data Protection and Privacy in the United States and Europe" (1998)

13

13

LAWS AND COMPLIANCE CONCEPTS

- Protect private information
- Notify individuals of breach
- Offline/Online content
- Sources:
  - Federal
  - State
  - Regulatory Dictates
  - Private Organizations *(PCI Security Standards Council)*

14

STATUTES IN THE UNITED STATES IMPACTING PRIVACY RIGHTS…

- Americans with Disabilities Act (ADA)
- Cable Communications Policy Act of 1984
- Children's Internet Protection Act of 2001 (CIPA) and Children's Online Privacy Protection Act of 1998 (COPPA)
- Communications Assistance for Law Enforcement Act of 1994 (CALEA)

15

15

STATUTES IN THE UNITED STATES IMPACTING PRIVACY RIGHTS…

- Computer Fraud and Abuse Act of 1986 (CFAA)
- Computer Security Act of 1987 *(subsequently superseded by the Federal Information Security Management Act (FISMA))*
- Consumer Credit Reporting Reform Act of 1996 (CCRRA)
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
- Electronic Funds Transfer Act (EFTA)

16

16

STATUTES IN THE UNITED STATES IMPACTING PRIVACY RIGHTS…

- Fair and Accurate Credit Transactions Act (FACTA) of 2003
- Fair Credit Reporting Act
- Federal Information Security Management Act (FISMA)
- Federal Trade Commission Act (FTCA)
- Driver's Privacy Protection Act of 1994
- Electronic Communications Privacy Act of 1986 (ECPA)

17

17

STATUTES IN THE UNITED STATES IMPACTING PRIVACY RIGHTS…

- Electronic Freedom of Information Act of 1996 (E-FOIA)
- Fair Credit Reporting Act of 1999 (FCRA)
- Family Education Rights and Privacy Act of 1974 (FERPA; also known as the Buckley Amendment)
- Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)
- Privacy Act of 1974

18

18

STATUTES IN THE UNITED STATES IMPACTING PRIVACY RIGHTS…

- Privacy Protection Act of 1980 (PPA)
- Right to Financial Privacy Act of 1978 (RFPA)
- Telecommunications Act of 1996
- Telephone Consumer Protection Act of 1991 (TCPA)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
- Video Privacy Protection Act of 1988

19

19

LAW AND COMPLIANCE CONCEPTS

State Data Breach Laws: According to the National Conference of State Legislators, 47 states and 4 territories have passed these laws

"Security breach laws typically have provisions regarding

- who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc);
- definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.);
- what constitutes a breach (e.g., unauthorized acquisition of data);
- requirements for notice (e.g., timing or method of notice, who must be notified); and
- exemptions (e.g., for encrypted information)."

20

WHY DATA BREACH NOTIFICATION LAWS?

NEWSDAY, April 28, 2005: "[ChoicePoint] announced in February that the personal information of 145,000 Americans may have been compromised when thieves posing as legitimate small business customers gained access to its database. Authorities say at least 750 people were defrauded in the scam."

21

21

IND. CODE 24-4.9-3-1

"[A] data base owner shall **disclose** [a] breach to an Indiana resident…if the data base owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in **identity deception** (as defined in IC 35-43-5-3.5), **identity theft**, or **fraud** affecting the Indiana resident.

22

22

IND. CODE 24-4.9-3-3.5

- A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner.

23

23

LAW AND COMPLIANCE CONCEPTS: THE EXAMPLE OF HIPAA

- HIPAA is the acronym for "The Health Insurance Portability and Accountability Act"
- Three main goals of HIPAA:
  - Reduce the administrative costs of healthcare,
  - Protect the privacy and insurability of individuals, and
  - Enhance safeguards against fraud and abuse.

24

24

AN EXAMPLE: HIPAA

What entities are covered?

- **Health Plans.** Insurers, HMOs, Medicare, Medicaid, group health plans (*).
- **Health Care Providers.** Hospitals, physicians, dentists…any health care provider who transmits health information in electronic form.
- **Health Care Clearinghouses.** Billing services, repricing companies, health networks.

25

25

AN EXAMPLE: HIPAA

HIPAA Covered Entity Requirements

1. **Privacy Policies and Procedures.** A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.
2. **Privacy Personnel.** A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.

26

26

AN EXAMPLE: HIPAA

Covered Entity Requirements

3. **Workforce Training and Management.**
   - Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of the entity (whether or not they are paid by the entity).
   - A covered entity must train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. A covered entity must have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.

27

27

AN EXAMPLE: HIPAA

Covered Entity Requirements

4. **Mitigation.** A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.

28

28

AN EXAMPLE: HIPAA

5. **Data Safeguards.** A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. (locks, shredding, etc.)
6. **Complaints.** A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule.

29

29

MORE FEDERAL LAW: THE FCRA

The Fair Credit Reporting Act (FCRA)

- 15 U.S.C. § 1681
- Enforced by the Federal Trade Commission
- Promotes accuracy in consumer reports
- Ensures the privacy of the information
- Amendments by the Fair and Accurate Credit Transactions Act of 2003

30

30

MORE FEDERAL LAW: THE FCRA

Consumers' basic rights under FCRA

- Notice of adverse action against consumer based on credit
- Disclosure of contents of file to consumer
- Disclosure of credit score to consumer
- Dispute rights
- 10 year limitation on information
- Limited access to file (especially employers and prospective employers)

31

31

MORE FEDERAL LAW: THE FCRA

The "Red Flag" Rule

- Each financial institution and creditor
  - that holds any consumer account,
  - or other account for which there is a reasonably foreseeable risk of identity theft,
- Must develop and implement an Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts.

32

32

MORE FEDERAL LAW: THE FCRA

The "Red Flag" Rule

- The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a financial institution or creditor to:
  - Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the Program;
  - Detect red flags that have been incorporated into the Program;
  - Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
  - Ensure the Program is updated periodically to reflect changes in risks from identity theft.

33

33

ONE LAST ONE: DPPA

Federal Law – Driver's Privacy Protection Act

- A state department of motor vehicles … shall not knowingly disclose or otherwise make available …
  - personal information about any individual obtained by the department … or
  - highly restricted personal information

34

34

ONE LAST ONE: DPPA

Federal Law – Driver's Privacy Protection Act

- Personal information, but not highly restricted personal information, may be disclosed for use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with:
  - claims investigation activities,
  - antifraud activities,
  - rating or underwriting.

35

35

ONE LAST ONE: DPPA

Federal Law – Driver's Privacy Protection Act

- "Personal information" means identifying information such a photograph, social security number, driver identification number, name, address (but not the 5- digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.
- "Highly restricted personal information" means an individual's photograph or image, social security number, medical or disability information

36

36

PRIVACY CONCEPTS IN THE INSURANCE INDUSTRY

37

AN EXAMPLE: NAIC CYBERSECURITY MODEL

1. The National Association of Insurance Commissioners (NAIC) has created a legal framework requiring insurance-related entities to implement and operate cybersecurity programs
2. NAIC model laws are suggestions for states to pass individually
3. NAIC developed this in hopes of getting a set of standardized laws countrywide

38

NAIC CYBERSECURITY MODEL

The National Law Review Reports:

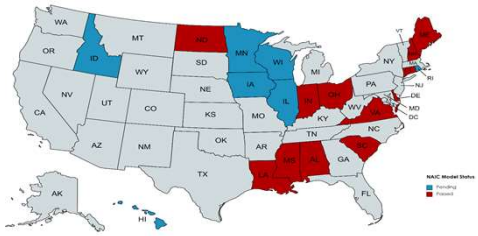
Maine and North Dakota Are Latest States to Adopt the NAIC Data Security Model Law

Thursday, April 15, 2021

Two more state governors, those of Maine and North Dakota, have signed bills into law that adopt the National Association of Insurance Commissioners (NAIC) data security model law (Model Law). Maine and North Dakota join several other states that have already passed similar laws. Hawaii, Idaho, Illinois, Iowa, Minnesota, Rhode Island, and Wisconsin have similar bills pending.

39

NAIC CYBERSECURITY MODEL – STATUS



40

NAIC CYBERSECURITY MODEL ACT

Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control…

41

NAIC CYBER SECURITY MODEL ACT

Have a "Program"

Develop, implement, and maintain a comprehensive risk-focused written Information Security Program, based on the licensee's risk assessment, that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information.

42

NAIC CYBER SECURITY MODEL ACT

Have someone in charge – a captain of the ship, so to speak

Designate one or more employees or an outside vendor and/or service provider designated to act on behalf of the Licensee who is responsible for the Information Security Program

43

THE BASIC PREMISE OF THE NAIC MODEL

Identify and Assess the Threats

- **Identify reasonably foreseeable internal or external threats** that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of Nonpublic Information;
- **Assess the likelihood and potential damage** of these threats, taking into consideration the sensitivity of the Nonpublic Information;

44

THE BASIC PREMISE OF THE NAIC MODEL

Review the Policies and Procedures

Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee's operations, including:

45

THE BASIC PREMISE OF THE NAIC MODEL

- ✓ Controlling access to the systems
- ✓ Restricting Physical Access
- ✓ Using encryption
- ✓ Testing Individual applications
- ✓ Training Employees
- ✓ Having an Incident Response Manual
- ✓ Stay current on threats
- ✓ Engage and utilize the Board of Directors

46

THE BASIC PREMISE OF THE NAIC MODEL

The regulated entity must also:

Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of Nonpublic Information, **including** the security of Information Systems and Nonpublic Information that are accessible to, or held by, **Third-Party Service Providers**

47

AND, FROM ACROSS THE POND COMES THE GDPR…

General Data Protection Regulation

1. Harmonization of data protection law across Europe
2. Applicable in UK despite Brexit (an important demonstration of "equivalence")
3. Greater obligations on data processors
4. Greater personal rights for data subjects, which are easier to enforce

Slide courtesy of: AXIS

48

THE NIST FRAMEWORK

- National Institute of Standards and Technology
- Part of the U.S. Department of Commerce
- "Framework for Improving Critical Infrastructure Cybersecurity"
- Version 1.1 issued April 16, 2018
- "The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks…"

49

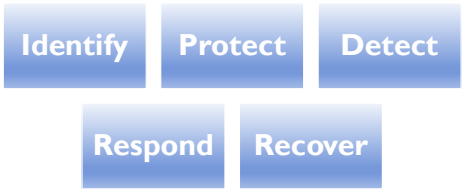
THE NIST FRAMEWORK

"[T]he Framework provides a common taxonomy and mechanism for organizations to:

1. Describe their current cybersecurity posture;
2. Describe their target state for cybersecurity;
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4. Assess progress toward the target state;
5. Communicate among internal and external stakeholders about cybersecurity risk."

50

THE NIST FRAMEWORK



The Framework Core Activities

51

CYBERSECURITY LAW IS A SWAMP OF LITIGATION AND REGULATORY DEVELOPMENTS

SECTION THREE

52

THE EXPERIAN CLASS ACTION SETTLEMENT

- A data breach is announced in 2015
- Affects more than 15 million consumers
- Plaintiffs allege compromised personal information, including addresses, social security numbers, military identification, and passport numbers.
- Plaintiffs also allege failure to protect data, failure to detect the breach, and failure of timely notice and disclosure

53

THE EXPERIAN CLASS ACTION SETTLEMENT

- The matter settles prior to class certification and is approved in the Central District of California in May of 2019
- The Court's order estimates the value as likely to exceed $170 million.
- Anticipated costs are: $138.8 million for credit monitoring; $22 for fees and costs; and $11.7 million for Experian's 60 new hires, enhanced encryption and revitalized security program.

54

STATE STATUTES AND REGULATIONS

California

- California is now creating regulations to implement the California Consumer Privacy Act of 2018 ("CCPA").
- CCPA became effective January 1, 2020.
- Enforcement through the Attorney General's office began in July, 2020.

55

STATE STATUTES AND REGULATIONS

California

- The CCPA applies to businesses in California:
  - With annual gross revenues exceeding $25 million;
  - Holding personal information of 50,000 or more consumers, households or devices; or
  - Earing more than half its annual revenue from selling consumer personal information.

Section 1798.140

56

STATE STATUTES AND REGULATIONS

CONCEPTUALLY,

- The CCPA shares some characteristics with the GDPR, such as:
  - A right to know what has been collected
  - A limited "right to be forgotten"

57

STATE STATUTES AND REGULATIONS

Biometric Data Protection

- Biometric laws now exist in Illinois, Texas, Washington and, soon, California.
- The laws generally grant data protection to identifiers like retinal scans, fingerprints, and facial geometry.

58

STATE STATUTES AND REGULATIONS

Rosenbach v. Six Flags Entertainment Corp., Case No. 2019 IL 123186, 2019 WL 323902 (Ill. Jan. 25, 2019).

- "[A violation of the Act] constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach.
- "[A] person or customer would clearly be 'aggrieved' within the meaning of section 20 of the Act and entitled to seek recovery under that provision.

59

STATE STATUTES AND REGULATIONS

Rosenbach v. Six Flags Entertainment Corp.,

"No additional consequences need be pleaded or proved. The violation, in itself, is sufficient to support the individual's or customer's statutory cause of action."

Large concern: the employment practices and/or human resources implications.

60

CYBERSECURITY LAW IS AN INSURABLE RISK (…WITH A FEW CAVEATS)

SECTION FOUR

61

THE COVERAGE QUESTION FROM SQUARE ONE

The CGL insuring clause reads:

We will pay those sums that the insured becomes legally obligated to pay as damages because of ***bodily injury or property damage*** to which this insurance applies. We will have the right and duty to defend any "suit" seeking those damages….

…caused by *an occurrence*…

62

62

THE COVERAGE QUESTION FROM SQUARE ONE

An "occurrence" is:

- ***"[A]n accident***, including continuous or repeated exposure to conditions which results in bodily injury or property damage…
- ***neither expected nor intended from the standpoint of the insured.***

63

63

THE COVERAGE QUESTION FROM SQUARE ONE

- Beyond "occurrence," the two main definitional hurdles are "bodily injury" and "property damage"
  - "Bodily injury" means bodily injury, sickness or disease sustained by a person, including death resulting from any of these at any time.

64

64

THE COVERAGE QUESTION FROM SQUARE ONE

- "Property damage" means:
  - ***Physical*** injury to ***tangible*** property, including all resulting loss of use of that property. All such loss of use shall be deemed to occur at the time of the physical injury that caused it; or
  - ***Loss of use*** of ***tangible*** property that is not physically injured…

65

65

SQUARE TWO?

- Previously, ISO had decided that electronic data was not tangible property – so, loss of use of data was not "property damage."
- In 2004, ISO added an exclusion to carve out coverage for "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."

66

66

SQUARE TWO?

The "New" CGL Language:

p. Electronic Data [This insurance does not apply to]

Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate ***electronic data.***

67

67

ISO'S LAWYERS PROFESSIONAL LIABILITY POLICY FORM

"Wrongful act" means any actual or alleged act, error or omission committed or allegedly committed by an "insured" which arises out of the rendering of or failure to render "*professional services*" and which resulted in actual or alleged damages.

68

ISO'S LAWYERS PROFESSIONAL LIABILITY POLICY FORM

"Professional services" means services rendered by an "insured" as an attorney, arbitrator, mediator, title agent, notary public, administrator, conservator, receiver, executor, guardian or trustee or in any other fiduciary capacity, provided such services, for which the insured is licensed, are *rendered in connection with the "named insured's" practice of law*.

69

69

WHAT CYBER / DATA BREACH INSURANCE LOOKS LIKE TODAY

70

70

HISTORY OF CYBER INSURANCE

- First policy was written in 1997
  - Hacker coverage only for third party suits
  - Failed to thrive and remained a niche for unusual demands
  - Long applications, high premiums, security reviews and restricted coverage
  - Long sales cycle
  - Only a couple carriers writing coverage

71

71

PRESENT DAY CYBER

- ***Fastest growing line of insurance***
  - Cyber insurance marketplace
    - Cyber premiums in 2008 = $500M, 2013 = $1.2B, 2014 = $2.4B
    - Projected to be $10B by 2020 and grow to $85B
    - Over 50 carriers now write the coverage
    - Lloyds is becoming Global Hub
    - Can provide indications with minimal information

72

72

What We're Insuring Against…

- 60% of small businesses close their doors within 6 months After a data breach
- They don't know what to do
  1. Compliance is a complicated process and involves several professionals.
  2. Must notify promptly or pay the price
  3. Reputational harm is devastating
  4. Cost to comply is expensive

73

73

WHAT WOULD YOU DO?

- It is a complicated process!
  - Forensics
  - Legal
  - Notification
  - Public Relations
  - Call Center
  - Credit Monitoring
  - Credit Restoration
- Fined if not reported ASAP.
  - Some states require reporting within 5 days
  - Fines are from $55k to $500k for late reporting

74

74

INSURANCE POLICY COMPOSITION

- The name does not matter –
- Add-on or Stand-alone
- Modular Policies – Build The Correct Coverage
- Basic insuring agreements
  - Risk Management, Third Party Coverage, First Party Coverage, Breach Response, Regulatory
  - Media coverage, Extortion - Crypto-ransomware infections have quadrupled since Q1 2014
- Options available
  - Business Income, Reputational harm, Errors & Omissions, Cyber crime, etc.

75

75

INSURANCE POLICY COMPOSITION

- Policy Type
  - Claims Made or Occurrence
  - Retro Dates or Full Prior Acts
  - One Aggregate Limit or Multiple
  - Notification on Dollar Amount or Record Count
  - Multiple Retentions or One
  - Co-Insurance, Waiting Period and Period of Indemnity
  - Indemnity Form or Pay on Behalf
  - Admitted or Non-Admitted
  - Duty to Defend or No

76

76

INSURANCE POLICY COMPOSITION

- **Risk Management Internet Module**
  - Risk Assessment Tools
  - Policies and Procedures
  - Vulnerability Testing
  - Monitoring of Known IP Addresses
  - Employee Training
  - Online Compliance and Breach Response Information
  - Newsletters and Email Notification About Key Legal and Regulatory Developments
  - Expert Phone or Online Support Online For Client Questions
  - Data Breach Coach
  - Incident Response Guides
  - Cyber Risk Webinars

77

77

INSURANCE POLICY COMPOSITION

- **Third Party Coverage**
  - **Network Security and Privacy Liability**
    - *Failure to prevent unauthorized access to, or use of private customer information on your computer system*
    - *Failure to prevent the transmission of a computer virus*
    - *Failure to provide notification to individuals of breach*
    - *Failure to prevent the participation of the insureds computer in a denial of service attack*

78

78

INSURANCE POLICY COMPOSITION

- **Possible Concerns**
  - ✓Employee and Corporate Information
  - ✓Accidental Release of PII
  - ✓Third Party Cloud Servers
  - ✓Information in Your Care Custody and Control

79

79

INSURANCE POLICY COMPOSITION

- **Third Party Coverage**
  - **Network Security and Privacy Liability**
    - **Possible Concerns - continued**
      - ✓ Breaches by third parties as well as rogue employees?
      - ✓ Breach of Contract or NDA
      - ✓ Service Provider Breaches
      - ✓ Electronic and Non-Electronic Information

80

80

INSURANCE POLICY COMPOSITION

- **Third Party Coverage**
  - **Regulatory Defense and Penalties**
    - *Pay on behalf of the insured claims expenses and penalties which the insured shall become legally obligated to pay because of any claim in the form of a regulatory proceeding*
    - **Possible Concerns**
      - ✓ Regulatory coverage. Violation of federal, state or local privacy laws?
      - ✓ Civil fines and penalties included in definition of damages?

81

81

INSURANCE POLICY COMPOSITION

- **Third Party Coverage**
  - **Payment Card Industry**
    - *To indemnify the Insured for PCI Fines, Expenses and Costs, in excess of the Retention, which the Insured shall become legally obligated to pay because of a Claim first made against any Insured during the Policy Period*
    - **Possible Concerns**
      - ✓ PCI approved forensic investigator
      - ✓ Affirmative coverage grant
      - ✓ Fines, penalties and assessments
      - ✓ Contractual coverage for breach of Merchant Services Agreements

82

82

INSURANCE POLICY COMPOSITION

- **Third Party Coverage**
  - **Website Media Content Liability**
    - *Damages and Claims Expenses … which the Insured shall become legally obligated to pay … for one or more of the following acts … in the course of the Insured Organization's display of Media Material on its web site or on social media …*
      - *defamation, libel, slander, infringement of copyright; infringement of domain name, trademark, trade name, trade dress, logo, title, metatag, or slogan, service mark, or service name; or improper deep-linking or framing within electronic content.*
    - **Possible Concerns**
      - ✓ How is media material defined?
      - ✓ Infringement of trademark included?
      - ✓ Website only?

83

83

INSURANCE POLICY COMPOSITION

- **Crisis Management Expense – First Party**
  - ✓Breach response vs. Indemnification
    - ✓ Coach, turnkey, panel or other?
  - ✓Forensics – *What about PCI Forensic Investigator?*
    - ✓ *Material risk of harm vs. legally liable*
  - ✓Legal Services to determine compliance

84

84

INSURANCE POLICY COMPOSITION

- **Crisis Management Expense – First Party**
  - ✓ Public Relations
  - ✓ Notification expense
    - ✓ Voluntary notification?
  - ✓ Call Center
  - ✓ Identity Restoration Counseling/Services
  - ✓ Credit Monitoring
    - ✓ How many agencies and for how long?

85

85

INSURANCE POLICY COMPOSITION

Options available

- Cyber Extortion
  - Ransom ware and DDoS
- Cyber Terrorism
  - Income loss from terrorist network shutdown
- Business Income
  - Waiting periods up to 24 hours
  - Ends when systems are back up

86

86

INSURANCE POLICY COMPOSITION

Options available

- Data Protection Loss
  - Costs to restore data from back-up or original
- Reputational Harm
  - Income loss from adverse notification
- Contingent BI/PD
- Errors & Omissions

87

87

INSURANCE POLICY COMPOSITION

- Options available
  - Cyber crime
    - Financial Fraud
      - Fraudulent instruction by third party sent to your bank to transfer funds pretending to be your or employee.
      - Fraudulent instruction from third party pretending to be you and asking an employee to transfer funds.

88

88

INSURANCE POLICY COMPOSITION

- Options available
  - Cyber crime
    - Phishing Attack Coverage
      - Fraudulent communications to impersonate you and your products/services in order to solicit personal and confidential information.
      - Covers your customers financial losses arising from attack.

89

89

G&G OIL CO. OF IN. V. CONT. WESTERN INS. CO.

"First, the interplay between computer fraud coverage and computer hacking is an emerging area of the law. Courts have had limited opportunities to construe these types of provisions. Second, computer hacking can take multiple forms. It can hardly be disputed that today's digital environment invites evolving degrees of cyber-malfeasance."

90

90

COVERAGE FOR HACKING (1)

G&G Oil Co. of Indiana v. Continental Western Insurance Company

- Indiana Court of Appeals
- March 31, 2020
- G&G suffers a ransomware attack and is unable to access servers and workstations.
- "Ultimately, G&G paid $34,477.50 for the four bitcoins it sent to the hijacker…. enabling it to decrypt its computers and regain access to its servers."

91

COVERAGE FOR HACKING (1)

- Continental Western's Commercial Crime Coverage Part form covers:

Computer Fraud

We will pay for loss of or damages to "money", "securities" and "other property" resulting directly from the use of any computer ***to fraudulently cause*** *a transfer of that property from inside the "premises" or "banking premises":*

a. To a person (other than a "messenger") outside those "premises"; or

b. To a place outside those "premises".

92

COVERAGE FOR HACKING (1)

The Court of Appeals says:

"Here, the hijacker did not use a computer to fraudulently cause G&G to purchase Bitcoin to pay as ransom. The hijacker did not pervert the truth or engage in deception in order to induce G&G to purchase the Bitcoin. **Although the hijacker's actions were illegal, there was no deception** involved in the hijacker's demands for ransom in exchange for restoring G&G's access to its computers. For all of these reasons, we conclude that the ransomware attack is not covered under the policy's computer fraud provision."

93

COVERAGE FOR HACKING (1)

On March 18, 2021, the Indiana Supreme Court says:

1. Targeted spear-phishing involves enough trickery to meet the common definition of "fraud," but,
2. We don't have proof that of this cause, and
3. "For example, if no safeguards were put in place, it is possible a hacker could enter a company's servers unhindered and hold them hostage. There would be no trick there."

94

COVERAGE FOR HACKING (1)

On March 18, 2021, the Indiana Supreme Court says:

4. G&G's transfer of Bitcoin resulted from use of a computer.
5. "G&G Oil's operations were shut down, and without access to its computer files, it is reasonable to assume G&G Oil would have incurred even greater loss to its business and profitability. These payments were 'voluntary' only in the sense G&G Oil consciously made the payment."

95

COVERAGE FOR HACKING (2)

Metal Pro Roofing, LLC v. Cincinnati Insurance Company

- Indiana Court of Appeals
- August 9, 2019
- Metal Pro's bank accounts were hacked and over $78,000 was stolen.
- Metal Pro wants coverage under the "Forgery or Alteration" or "Inside the Premises – Theft of Money and Security" coverages of the Expanded Coverage Plus Part of the Crime policy.

96

COVERAGE FOR HACKING (2)

On the Forgery claim:

- "The policies define 'forgery' as 'the signing of the name of another person or organization with intent to deceive[.]' [The Insured does] not cite any evidence that the hacker 'signed' anything, let alone that they signed 'the name of another person or organization.'"

On the "Inside the Premises" claim:

- "That coverage applies to losses resulting directly from ``theft' committed by a person present inside [the business's] `premises' or `banking premises[.]"
- "[The Insured does] not direct us to any evidence that the person who committed the thefts was inside the LLCs' building(s) or a bank building."

97

COVERAGE FOR HACKING (2)

- HOWEVER, Cincinnati's promotional materials said, among other things:

*Cincinnati can insure your money and securities while at your premises, inside your bank and even off site in the custody of a courier. While you've taken precautions to protect your money and securities, you run the risk of loss from employees, robbers, burglars, **computer hackers** and even physical perils such as fire.*

The Court of Appeals says:

"It would be entirely reasonable for a prospective insured to read that language, in that sequence, to mean, 'If you want to be covered for theft by computer hackers, you should buy this endorsement.'"

98

BUT SO FAR, THE BIGGEST COVERAGE RISK HAS BEEN SOCIAL ENGINEERING

- Medidata Solutions, Inc. v. Federal Insurance Company, United States Court of Appeals for the Second Circuit, No. 17-2492-cv (July 6, 2018)
- American Tooling Center, Inc. v. Travelers Casualty and Surety Co., United States Court of Appeals for the Sixth Circuit, No 17-2014 (July 13, 2018)

99

BUT THE NEXT ONE MAY BE THE "ACTS OF WAR" EXCLUSION

Mondelēz International

Was the NotPetya cyber attack a "hostile or warlike action… by any government or sovereign power … or agent or authority…"?

ZURICH

100

INFORMATION SECURITY: A PLAN TO PROTECT YOUR AGENCY

Task Force Developed Program

- Exclusive Membership Benefit
- Up to 50% premium reduction
- Box rated
- Simple application process
- Educational
- Risk Management Module
- First Party and Third Party Coverage

101

COMPANIES WITH < $1,000,000 IN REVENUES

	Option 1	Option 2	Option 3
Limit of Liability	$250,000	$500,000	$1,000,000
Retention	*$2,500*	*$2,500*	*$2,500*
Notification Limit (outside limit of liability)	25,000 records	25,000 records	25,000 records
Notification Threshold	*100 Records*	*100 Records*	*100 Records*
Sublimits			
Regulatory Defense & Penalties	$250,000	$500,000	$1,000,000
PCI Fines & Penalties	$50,000	$50,000	$50,000
Website Media Liability	$250,000	$500,000	$1,000,000
Cyber Extortion	$250,000	$500,000	$1,000,000
Legal & Forensics	$250,000	$250,000	$250,000
Public Relations	$100,000	$100,000	$100,000
Fraud Resolution	5,000 records	5,000 records	5,000 records
Premium less than 50% benefits	**$250.00**	**$500.00**	**$750.00**

102

COMPANIES WITH REVENUES FROM $1M TO $2M

	Option 1	Option 2	Option 3
Limit of Liability	$500,000	$1,000,000	$1,000,000
Retention	*$2,500*	*$2,500*	*$2,500*
Notification Limit (outside limit of liability)	25,000 records	25,000 records	50,000 records
Notification Threshold	*100 Records*	*100 Records*	*100 Records*
Sublimits			
Regulatory Defense & Penalties	$500,000	$1,000,000	$1,000,000
PCI Fines & Penalties	$50,000	$50,000	$50,000
Website Media Liability	$500,000	$1,000,000	$1,000,000
Cyber Extortion	$500,000	$1,000,000	$1,000,000
Legal & Forensics	$250,000	$250,000	$250,000
Public Relations	$100,000	$100,000	$100,000
Fraud Resolution	5,000 records	5,000 records	5,000 records
Premium less than 50% benefits	**$550.00**	**$850.00**	**$950.00**

103

COMPANIES WITH REVENUES FROM $2M TO $3M

	Option 1	Option 2	Option 3
Limit of Liability	$500,000	$1,000,000	$1,000,000
Retention	*$2,500*	*$2,500*	*$2,500*
Notification Limit (outside limit of liability)	25,000 records	25,000 records	50,000 records
Notification Threshold	*100 Records*	*100 Records*	*100 Records*
Sublimits			
Regulatory Defense & Penalties	$500,000	$1,000,000	$1,000,000
PCI Fines & Penalties	$50,000	$50,000	$50,000
Website Media Liability	$500,000	$1,000,000	$1,000,000
Cyber Extortion	$500,000	$1,000,000	$1,000,000
Legal & Forensics	$250,000	$250,000	$250,000
Public Relations	$100,000	$100,000	$100,000
Fraud Resolution	5,000 records	5,000 records	5,000 records
Premium less than 50% benefits	**$750.00**	**$950.00**	**$1100.00**

104

COMPANIES WITH REVENUES FROM $3M TO $4M

	Option 1	Option 2	Option 3
Limit of Liability	$500,000	$1,000,000	$1,000,000
Retention	*$2,500*	*$2,500*	*$2,500*
Notification Limit (outside limit of liability)	25,000 records	25,000 records	50,000 records
Notification Threshold	*100 Records*	*100 Records*	*100 Records*
Sublimits			
Regulatory Defense & Penalties	$500,000	$1,000,000	$1,000,000
PCI Fines & Penalties	$50,000	$50,000	$50,000
Website Media Liability	$500,000	$1,000,000	$1,000,000
Cyber Extortion	$500,000	$1,000,000	$1,000,000
Legal & Forensics	$250,000	$250,000	$250,000
Public Relations	$100,000	$100,000	$100,000
Fraud Resolution	5,000 records	5,000 records	5,000 records
Premium less than 50% benefits	**$950.00**	**$1100.00**	**$1250.00**

105

COMPANIES WITH REVENUES FROM $4M TO $5M

	Option 1	Option 2	Option 3
Limit of Liability	$1,000,000	$1,000,000	$1,000,000
Retention	*$2,500*	*$2,500*	*$2,500*
Notification Limit (outside limit of liability)	25,000 records	50,000 records	100,000 records
Notification Threshold	*100 Records*	*100 Records*	*100 Records*
Sublimits			
Regulatory Defense & Penalties	$1,000,000	$1,000,000	$1,000,000
PCI Fines & Penalties	$50,000	$50,000	$50,000
Website Media Liability	$1,000,000	$1,000,000	$1,000,000
Cyber Extortion	$1,000,000	$1,000,000	$1,000,000
Legal & Forensics	$250,000	$250,000	$250,000
Public Relations	$100,000	$100,000	$100,000
Fraud Resolution	5,000 records	5,000 records	5,000 records
Premium less than 50% benefits	**$1200.00**	**$1350.00**	**$1500.00**

106