CNA

Everyone’s Nightmare: Privacy and Data Breach Risks

May 1, 2014

Edwards Wildman Palmer, LLP
Privacy & Data Protection Group

Laurie A. Kamaiko
New York Office
lkamaiko@edwardswildman.com

Thomas J. Smedinghoff
Chicago Office
tsmedinghoff@edwardswildman.com
Agenda

1. Cyber Risks and Exposures
2. US Legal and Regulatory Framework
3. Breach Response: The Drivers and How to Control Them
4. Litigation Trends
5. Insurance Products: Scope and Limitations
1. Cyber Risks and Exposures
2013 – “The Year of the Mega Breach”

Who is at Risk for Data Breaches: Industries Most Affected

- Retail - 31% POS; 10% web app attack; 33% Denial of Service – Verizon 2014
- Accommodation - 75% POS intrusions in 2013 – Verizon 2014 Report
- Financial services (including insurance)
- Healthcare – 43% reported breaches in 2013 (IDTheftCenter.org)
  - 100% increase in criminal attacks on healthcare systems since 2010; increase in breach risks from personal unsecured devices (Ponemon, Study on Patient Privacy & Data Security, 3/2014)
- Educational institutions
- Government entities
- IT/Technology entities
- Entertainment (online)
- Any entity with Personal Information/Data of own employees or customers/clients
- Manufacturing when target information is trade secrets
Data Breaches

♦ **Personal Information (PI)**
  ◆ Information about individuals defined by statutes and regulations
  ◆ Heavily regulated to protect against identity theft and fraudulent transactions
  ◆ Special rules for –
    ◇ Non-public Personal Information (NPI) – financial sector
    ◇ Protected Health Information (PHI) – healthcare sector
    ◇ Information about children

♦ **Corporate financial information**

♦ **Other confidential corporate information**
  ◆ Corporate trade secrets
  ◆ Other Intellectual Property
  ◆ Business secrets
  ◆ Client/customer secrets
Other Cyber Incidents

- Cyber attacks on property and business functions
  - Denial of service attacks/disruption of operations
  - Zombies
  - Website defacement
  - Other forms of mischief
- Extortion / Hacktivism
- Terrorism and Attacks against Critical Infrastructure
Business Practices re Personal Information

- Increasing regulation → increasing liability
- Issues include:
  - Collection and usage of information about individuals
  - Sharing of Information
  - Online behavior tracking (cookies, etc.)
  - BIG DATA
  - The “Internet of Things”
  - Disclosure of practices
- Are you compliant regarding –
  - Collection, usage and disclosure practices?
  - Privacy policies on websites?
  - Online apps?
- Risk that what is compliant today is not compliant tomorrow
Other Risks and Exposures

♦ Use of cloud service providers and other vendors
  ♦ access to company data
  ♦ avenue for malware intrusion
  ♦ lack of control
  ♦ Indemnity provisions

♦ Incorporating use of personal devices and social media into workplace
  ♦ BYOD/BYOC/BYOx
  ♦ Social Media

♦ Developing National / Industry Standards – e.g., CSF
♦ Expansion of statutory liabilities
♦ Increased Regulatory Enforcement
♦ Contractual responsibilities → liabilities
Sources of Risks

Sources of and Responsibility for Breaches
- Lost/stolen mobile devices
- Third Party Vendors
- Systems failure

Criminal/Malicious Activity
- Rogue employees
- External hackers

Negligence
- Internal
- External
**Recent Studies of Reported Breaches Show:**

<table>
<thead>
<tr>
<th>Cause of Breaches in 2012:</th>
<th>For payment card breaches, in 99% someone else told victim organization they had suffered a breach; often, customers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>37% - Malicious or criminal attack</td>
<td>37% - Malicious or criminal attack</td>
</tr>
<tr>
<td>35% - Negligent employee</td>
<td>35% - Negligent employee</td>
</tr>
<tr>
<td>29% - System glitch</td>
<td>29% - System glitch</td>
</tr>
</tbody>
</table>

**2013 Ponemon Institute**

<table>
<thead>
<tr>
<th>&quot;Everyone is vulnerable to some type of event” - if not external attack, than insider misuse/errors that expose data and harm systems</th>
<th>In 2013 DDOS attacks increased in size and frequency: application layer attacks rose 42% and infrastructure attacks rose 30%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over 25% of stolen data in 2012 was encrypted by cybercriminals.</td>
<td>50% of 2013 breaches studied by Verizon took months or longer to discover; once discovered, entities take days or less to respond</td>
</tr>
</tbody>
</table>

**2014 Verizon Data Breach Investigations Report**

<table>
<thead>
<tr>
<th>76% of network intrusions in 2012 exploited weak or stolen credentials. 2013 showed increase in use of stolen credentials.</th>
<th>Malware targeting Android mobile operating systems increased by 400% in 2012.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase in external actors in 2013, up from 2012, with decrease in financial motive and increase in espionage</td>
<td>Increase in external actors in 2013, up from 2012, with decrease in financial motive and increase in espionage</td>
</tr>
</tbody>
</table>

**2014 Verizon Data Breach Investigations Reports**

|----------------------------------------------------------|----------------------------------------------------------|

---

*Edwards Wildman*
2013 STATS AND TRENDS

- 91% increase in targeted attacks
- 62% increase in number of breaches
- 1 in 392 emails contains a phishing attack
- Web based attacks up 23%
- 1 in 8 legitimate websites has a critical vulnerability
- US is ranked No. 1 for malicious activity

*From Symantec  2014 Internet Security Threat Report*

- Transition from geopolitical attaches to large scale payment systems attacks (retailers)
- Increase in insider espionage targeting internal data and trade secrets
- Increase in internal discovery of breaches

*From Verizon 2014 Data Breach Investigations Report*
Cost of Data Breaches

Cost of Data Breach:
- Average cost of US data breach was over $5.4 million
- $188 per record exposed.

Factors That Reduced Cost:
- Incident Response Plan – reduced cost $42/record
- Strong Security Posture – reduced cost $34/record
- Chief Information Security Officer (“CISO”) – reduced cost $23/record
- Outside consultant assisting in response – reduced cost $13/record

Factors that Increased Cost:
- Too quick a notification – increased cost $37/record
  - But delays in notification can be major issue in regulatory and media scrutiny, as well as class action lawsuits

Cost Data – Insured Claims

Cost of a Data Breach based on **insured** claims data for 140 events/88 claim payouts between 2010 and 2012*

- Cost per record: median $99; average $307 (excluding outliers)
- Claim payout - median $242,500; average $954,253
  - Smallest – $92,560; Largest - $20 million
- Crisis services (forensics, notification, audit monitoring, legal guidance) median $209,625; average $737,213
- Legal Defense: median - $7,500; average - $574,900, range 0 > 10 million
- Legal Settlements: median - $22,500; average - $50,099
- Forensic Cost Range: $ 0 - $1 million
- Notification Cost Range: $0 to $3 million
- Credit monitoring and identity theft remediation: $0 - $935,000

* Source: Net Diligence 2013 Cyber Liability & Data Breach Insurance Claims: A study of Actual Claim Payouts
Cost Categories

Direct Costs
- Crisis Management
- Mandatory notifications
- Legal advice
- Contractual penalties
- Remediation
  - To consumers, e.g. credit monitoring and theft insurance
  - To own systems

Civil Liability
- Breach of Contract
- Breach of Confidentiality
- Third Party Claims
- Legal Fees

Regulatory Liability
- Investigation and/or Audit Costs
- Regulatory Fines
- Also involve legal fees

Reputation Management
- Marketing and PR
- Voluntary notifications
- Remediation Services other than those required

Business Disruption
- Denial/Disruption of services
- Management Resources
- Impairment of Equipment

Indirect Costs
- Customers/Business
- Reconstitution of Data
- Loss of Profits/Earnings
2. US Legal and Regulatory Framework
Two Basic Data Security Legal Obligations

♦ Duty to **protect**
  ♦ Provide “reasonable” security for corporate data and systems

♦ Duty to **disclose**
  ♦ Disclose breaches (to affected parties and regulators)
  ♦ Disclose material risks

♦ Both duties are continually expanding in scope!
Where Do These Obligations Come From?

- A patchwork of Statutes and Regulations
  - Security laws and regulations (mostly state level)
  - Privacy laws
  - E-transaction laws
  - Corporate governance legislation and regulations (e.g. SOX)
  - Unfair business practice laws and enforcement thereof
  - Sector-specific laws/regulations, such as HIPAA, GLB, SEC, FTC, SOX, etc.

- Common Law Obligations
- Rules of Evidence
- Contractual Obligations
- Industry Self-Regulation
- Self-Imposed Obligations
What Do These Obligations Apply to?

- Systems and networks
  - Physical facilities
  - Hardware devices (including cloud, BYOD, etc.)
  - Software (e.g., Heartbleed)
  - Communications networks

- Data storage media
  - Online and offline
  - Fixed and removable/moveable (e.g., laptops, flash drives)

- Data
  - Personal data
  - Intellectual property
  - Confidential corporate information – e.g., corp. financial data
  - Corporate documents and communications

- Other
2a. The Duty to Protect: i.e., Duty to Implement Reasonable Security
Objectives of Data Security

♦ Protect systems, media, and data

♦ Goals to be achieved --
  ♦ Ensure confidentiality
  ♦ Ensure integrity
  ♦ Ensure availability

♦ Harms to be avoided –
  ♦ Unauthorized access, use, disclosure or transfer, modification, alteration, or processing
  ♦ Accidental or intentional loss or destruction
Categories of Security Measures

- **Physical**
  - Examples include: fences, walls, and other barriers; locks, safes, and vaults; armed guards; sensors and alarm bells

- **Technical**
  - Examples include: firewalls, intrusion detection software, access control software, antivirus software, passwords, smart cards, biometric tokens, and encryption processes

- **Administrative**
  - Examples include: personnel management, employee use policies, training, and discipline
The Legal Standard – Reasonable Security

♦ Must implement “appropriate” measures to protect data
  ♦ U.S. – Privacy Act of 1974, GLB, HIPAA, several state data security laws
  ♦ EU Data Protection Directive

♦ Must implement “reasonable” measures to protect data
  ♦ Several state data security laws
  ♦ E.g. - “A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.” Cal. Civ. Code § 1798.81.5(b).

♦ The legal standard recognizes that security is a relative concept.
Defining “Reasonable” Security

✧ Two leading approaches – both very similar

✧ **Comprehensive written information security program (WISP)**
  ✧ GLB security regulations (Fed, OTC, FDIC, OCC) – 2001
  ✧ GLB security regulations (FTC) – 2002
  ✧ FTC enforcement actions – 2002–present
  ✧ FISMA (gov’t agencies) – 2002
  ✧ HIPAA security regulations (HHS) – 2003
  ✧ Oregon (as a safe harbor) – 2007
  ✧ Massachusetts regulations – 2008
  ✧ AG enforcement actions and developing case law
  ✧ International - EU Data Protection Directive, Argentina, Austria, Iceland, Italy, Netherlands, Norway, Philippines, Poland, Portugal, Spain, and others

✧ **NIST Cybersecurity Framework**
  ✧ Voluntary framework released by NIST February 12, 2014
  ✧ Based on consensus of public-private collaboration
  ✧ May ultimately become a de facto legal standard
A WISP Requires a “Process” . . .

- Assign responsibility
- Identify the information assets to be protected
  - Both (i) under company control and (ii) outsourced
- Conduct risk assessment
  - Identify and evaluate threats, vulnerabilities, and damages
- Select, develop & implement security controls --
  - That are responsive to the risk assessment
  - That address the required “categories” of controls
- Address third party issues
- Continually monitor the effectiveness of the program
- Regularly review, reassess, and adjust the program
to Determine Appropriate Security Controls within Specified “Categories”

- Physical controls
  - Facility and equipment
  - Media

- Technical controls
  - Access controls
  - Identification and authentication
  - System configuration and change management
  - System and information integrity
  - Data communications protection
  - Maintenance
  - System activity monitoring

- Administrative Controls
  - Personnel security
  - Employee awareness and training
  - Backup and disaster planning
  - Incident response planning
The New “Cybersecurity Framework” Takes a Similar Approach

- Released by the federal government on February 12, 2014
- Proposed as a voluntary best practice guide
- Aimed at critical infrastructure organizations but written to apply to any entity
- Takes a very similar (but expanded) approach, via five functional categories –
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
2b. The Duty to Disclose:
i.e., Duty to Notify of Security Breaches
Overview of State Breach Notification Laws

- Basic concept – Breach of covered information requires notice to affected persons

- Not a new concept
  - Appears in IRS regulations for tax data

- Started in California in 2003 for personal information
  - Now 47 states (plus DC, US VI and PR)
  - Several other countries

- Obligation akin to common law “duty to warn”

- Applies to breaches of sensitive personal information

- Having a major PR impact
State Breach Notification Requirements (1)

♦ Covered information (varies by state) -- basic formulation is --
  - “Name” plus
  - Any one of the following:
    - SSN
    - Drivers license or government issued ID number
    - Financial account or credit card number
    - Other (e.g., healthcare data in some states)

♦ Triggering event (varies by state)
  - Any breach of security, or
  - Only breaches with reasonable likelihood of harm
  - Definition of “breach” varies by state; encryption is a safe harbor

♦ Your obligations if a breach occurs
  - Investigate and remedy problem – (some states)
  - Notify persons whose information compromised
  - Notify state enforcement agencies – (some states)
  - Notify credit agencies – (some states)
State Breach Notification Requirements (2)

- **Timing of the notice**
  - In the “most expedient time possible and w/o unreasonable delay”
  - Delay usually OK for law enforcement investigation or to take necessary measures to determine the scope of the breach and restore system integrity

- **Form of notice**
  - In writing (i.e., paper and first class mail)
  - Electronic form (but must comply with E-SIGN)
  - Substitute notice, if affected persons unknown or volume and cost thresholds met conditions met (general publication by press, website, etc.)
  - Alt (some states) – follow company incident response plan

- **Content of notice (varies by state)**

- **Penalties**
  - State enforcement (e.g., AG office)
  - Some private right of action

♦ Gramm-Leach-Bliley Act (applies to financial institutions broadly defined)
  ♦ Breach notification required by regulation

♦ HIPAA and HITECH (applies to health and medical information in certain circumstances)
  ♦ Breach notification required by statute and regulation

♦ FTC Red Flags

♦ Other privacy statutes, including Fair Credit Reporting Act, Video Privacy Protection Act, Children’s Online Privacy Protection Act, Family Educational Records Privacy Act, etc.
Public companies must disclose *material events* which a reasonable investor would consider important to an investment decision.

Guidance: Registrants should disclose material cybersecurity *risks* and *incidents*:

- Requires risk assessment
  - Internal and external threats
  - Identity vulnerabilities
  - Likelihood of threats exploiting vulnerabilities
  - Impact/damage
  - Adequacy existing security
- Avoid generic risk disclosure; describe material risks and specify how each affects the company
- Identify outsourcing that has material risk and how addressed
- Describe known or threatened cyber incidents
- Guidance also refers to describing relevant insurance
Credit/Debit Cards – PCI Standards

♦ PCI DSS (Payment Card Industry Data Security Standard)
  ♦ Contract-based obligation applicable to anyone who accepts credit cards
  ♦ Requires specified security measures to protect credit card transactions
  ♦ Requires reporting of breaches to credit card companies
  ♦ Also incorporated into some state statutes (e.g. NV, MN, WA) and in regulatory scrutiny and fines assessments by some AGs

♦ Major factor in any credit/debit card breach
  ♦ Only 10% of organizations were fully compliant with PCI at time of baseline assessments (Verizon 2014 PCI Compliance Report)

♦ Liability impact
  ♦ Breached merchants are contractually liable for assessments imposed by Card Brands for PCI DSS violations, fraudulent charge reimbursements, card replacement/monitoring and administrative costs of card issuers.
  ♦ Basis of negligence and other allegations in third party claims
  ♦ Recent attempts by some banks/credit unions to sue breached entities for financial losses from and breaches not reimbursed through PCI system
Federal and State Enforcement Trends

♦ Actions are more numerous, reaching smaller breaches and resulting in larger settlements

♦ Enforcement focused on companies that --
  ♦ knew or should have known of a problem,
  ♦ ignored legal, regulatory and PCI requirements
  ♦ Inadequate security procedures, training, risk assessments

♦ FTC enforcement focused on unfair and deceptive trade practices
  ♦ “Unfair” is having inadequate security
  ♦ “Deceptive” is acting out of conformance with policies and statements
  ♦ April 2014 – decision in FTC v. Wyndham Worldwide (D.N.J.) – confirmed FTC has authority to regulate data security under “unfairness” prong despite lack of formal rules or regulations setting standards

♦ Impact of FTC enforcement -
  ♦ Basic GLB/HIPAA obligations extended to non-regulated businesses
  ♦ Protection extended beyond breach notification data to all consumer data, including log-in credentials (Twitter) and Facebook postings

♦ Healthcare is increasingly active by both Health and Human Services and states, which now have ability to enforce HIPAA/HITECH
3. Breach Response:
The Drivers and How to Control Them
Legal, Regulatory & Contractual Obligations

♦ Know what they are in Advance
  ♦ What legal and regulatory requirements, and what contracts are implicated?
    ♦ The time to inventory and review contracts, and to catalogue applicable requirements is in advance.
  ♦ Contracts beyond PCI
    ♦ Financing agreements
    ♦ Investors’ agreements
    ♦ Vendor contracts
Jurisdictional and International Issues

♦ Content, Timing and Format of Notice
  ♦ Mail hardcopy in US
  ♦ Email often acceptable or preferred in other countries
  ♦ Substitute notice
    ♦ Publication and Media notice
    ♦ Email
    ♦ Website posting
  ♦ Differences in Remediation offerings
  ♦ Call center capabilities
Forensics Investigations

♦ Engaging outside investigators – in advance
  ♦ Costs can be highly significant
  ♦ Advance planning and consultation
  ♦ Outside resources can be important
  ♦ Negotiated costs
  ♦ Advice to mitigate exposure and expense

♦ Determining what Happened; Possibly Ruling out a Breach

♦ Challenges that extend Timeframes and drive up Costs
  ♦ Unstructured Databases
  ♦ Record Retention Issues
  ♦ Searchability of PHI
  ♦ Access Logs
  ♦ Payment Card Industry (PCI) requirements
  ♦ Vendors and Sub-Vendors
Notification Costs – Beyond Printing and Postage!

♦ How clean and current is the database?
  ♦ Consider the condition of the database in advance
    ♦ De-duping the mailing list
  ♦ Determining who gets notice
  ♦ Composing the letters to comply with varying and sometimes conflicting requirements, and to set the right tone.
  ♦ How customized are the letters; how many versions are involved?
    ♦ PHI and PI combined
Remediation Costs & Risk Mitigation

♦ Remediation Costs
  ♦ Choosing the appropriate level of service
    ♦ Higher level of service equals higher cost, but also more favorable response

♦ Risk Mitigation Steps
  ♦ Outside resources can be helpful and add credibility
  ♦ Risk assessment, including penetration testing
  ♦ Qualified Security Assessor may be required by credit card industry, but there are costs and benefits to independence
  ♦ Evaluate contractual and common law indemnity that may be available
4. Litigation Trends
Litigation Trends

♦ Litigation arising from breaches of PI
  ♦ Failure to adequately secure information
    ♦ Litigation 2x more likely if breach perceived as from carelessness vs. company inability to prevent (Draft Study, Cy Labs of Carnegie Mellon)
  ♦ Failure to adequately respond to breach
  ♦ Untimely notice
  ♦ Misrepresentation of cause, effect
  ♦ Violation of consumer protection statutes
  ♦ > 80 different causes of action have been identified

♦ Financial Incentives of Litigation
  ♦ U.S. Consumer Class Actions
    ♦ Driven by financial incentive vs. challenge of proving legally cognizable damages
    ♦ Trend of asserting “lost value”
      ♦ Of stolen passwords and user names
      ♦ Of portion of service fee that is for security
      ♦ Of loss of use of service or computer
Bases of Potential Liability

♦ Failure to provide reasonable security for breached information
  ♦ Inadequate security
  ♦ Misrepresentation of security
  ♦ Failure to warn of inadequate security

♦ Failure to adequately respond to breach
  ♦ Failure to notify
  ♦ Untimely notification
  ♦ Misrepresentation of cause or effect
  ♦ Violation of consumer protection statutes
    ♦ 80 different causes of action identified
Potential Parties in Data Breach cases

♦ Potential Plaintiffs
  ♦ Consumers whose PI is accessed (consumer class actions)
  ♦ Financial institutions affected (fraud charges, card replacement costs, etc.)
  ♦ Shareholder/derivative suits
    ♦ Share price drops
    ♦ Board approval of inadequate security
    ♦ Misrepresentation/failure to disclose: cause, timing of disclosure, information at risk, etc.
  ♦ Breached entity seeking contribution from vendors, others responsible for lapse in security, etc.
  ♦ Regulators (e.g., FTC, state AGs, etc.)

♦ Potential Defendants
  ♦ Breached entities
  ♦ Vendors holding PI or involved in security or design
  ♦ Vendors who assisted in data security assessments or remediation
  ♦ Professional advisors
  ♦ D & Os approving company security policies, responses and financial disclosures
  ♦ Vendors
Threshold Issues: What are Compensable Injuries

- **Standing in federal court**
  - Federal jurisdiction requires “case or controversy” → injury in fact that is actual or imminent, not conjectured or hypothetical

- **Cognizable injury under state law**
  - Does law provide a remedy for alleged injury
  - What is no identity theft or out-of-pocket financial loss

- **Theories asserted to avoid dismissal for lack of injury include:**
  - Consumer protection statute violated → statutory damages
  - Misrepresentation in privacy policy re security
  - Price for service provided to consumer included data security, and that not delivered
Litigation Trends: Other Privacy Litigation

- New Theories of Liability for Non-Breach Lawsuits
  - Online behavioural advertising/consumer tracking
    - Improper collection practices
    - Improper disclosures
  - Statutory violations that are not data breaches per se
  - Privacy Violations - Wrongful collection and usage of information/Disclosure Practices
    - Wrongful collection/sale of PI
    - Zip Codes as PI when requested by retailers without need (California, Massachusetts, and possibly other states soon)
    - Compliance with disclosure of collection/sharing – e.g. California Share the Light
    - Adequacy of privacy policies and company compliance with representations in privacy policies
    - Unauthorized Distribution (Blasting – e.g. TCPA)
  - Statutory restrictions on recording business calls with consumers
  - Trend toward asserting violations of unfair trade practices statutes and consumer protection statutes and seeking statutory damages.
5. Insurance Products: Scope and Limitations
Specialty Insurance Policies/Endorsements ("Cyber/Privacy/Network Security")

♦ Coverages generally designed to apply to first party losses as well as third party claims
♦ Types of Coverages (but not all policies offer all options):
  ♦ Personal information/privacy coverages
  ♦ Expansion to other types of “confidential information”
  ♦ Network security
  ♦ Cyber extortion
  ♦ Business disruption/interruption from breach or attack
  ♦ Digital asset damage/loss
  ♦ Technology E&O
  ♦ Wrongful collection/usage of PI / disclosures of usage
♦ Terms and Scope of coverages vary
♦ Often limitations on coverage, including sublimits and/or exclusions
♦ Increasing demand for such policies
  ♦ Recognition of exposures
  ♦ Increasingly contractually required
  ♦ U.S. SEC Guidance advises disclosure of pertinent insurance
## Cyber/Privacy/Network Security

### Some Stress Points:

<table>
<thead>
<tr>
<th>First Party Cost</th>
<th>vs.</th>
<th>3rd party claim expense/mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Required notification/remediation</td>
<td></td>
<td>voluntary (but customary); arguably mitigates against likelihood of 3rd party claims/damages</td>
</tr>
<tr>
<td>Prior consent requirement</td>
<td></td>
<td>need for immediate retention of forensics and other vendors</td>
</tr>
<tr>
<td>PCI “fine or penalty”/contractual assessment/liquidated damages exclusions</td>
<td></td>
<td>damages would be liable for in absence of contract</td>
</tr>
<tr>
<td>Permissible conduct at time of act</td>
<td></td>
<td>impermissible at time of claim</td>
</tr>
<tr>
<td>Malware discovered during one policy year (1st party coverage trigger)</td>
<td></td>
<td>claim made against insured in subsequent policy year (3rd party coverage trigger)</td>
</tr>
<tr>
<td>Not cover upgrades</td>
<td></td>
<td>improved security reduces risk of continuing breach and likelihood of subsequent event</td>
</tr>
<tr>
<td>Cover Business Losses</td>
<td></td>
<td>How determine amount of loss due to covered event</td>
</tr>
</tbody>
</table>
How “Cyber” Policy Wordings Make a Difference When There is a Data Breach – Some Examples:

- Trigger Language – and coordination between 1st and 3rd party coverages
- Covered Costs: investigation, response, remediation, extra expense/mitigation of third party claims, asset replacement, business income losses
- Consent Provisions
- Definitions
  - Your Network/Computer – include vendors, cloud providers, employees?
  - Damages…and carve outs from Damages
  - Fines and Penalties
- Importing traditional exclusions into Cyber Risk Policies
  - Contractual Liability, etc.
- Sublimits: Pros & Cons
- Security Standard Requirements
Traditional Lines of Coverage

General Liability (Third Party Claims only)
- Bodily injury or property damage
  - Subject to electronic data and other exclusions
    - New endorsements in US directed at excluding claims regarding Access or Disclosure of PI, some with exception for bodily injury
  - Data not “tangible property”, but loss of use of hardware argued to be Property Damage
  - US: Duty to defend broader than duty to indemnify, so allegations can trigger defense costs

Personal Injury and Advertising Injury Coverage
- Usually includes offense of injury arising out of:
  - “. . .publication, in any manner, of material that violates a person’s right of privacy”
- New US optional endorsement deletes this prong, reducing exposure)
- Are statutory assessments “Damages”? Fines or Penalties?
- Exclusions for breach related claims being issued
Other Traditional Lines of Coverage:

- Property (if tangible property/loss of use involved)
  - Valuable Papers (sublimits)
  - Loss of use, e.g., property damage and disruption of operations
  - Business Interruption/Contingent Business Interruption
  - Scope of exclusions sufficient to preclude coverage?

- Kidnap & Ransom (cyber extortion)

- Professional liability (which often have Cyber Endorsements)
  - Lawyers, healthcare, accountants, real estate agents, A&E, etc.

- Technology and other E&O: service providers, product developers
Other Traditional Lines of Coverage:

♦ Crime / Fidelity
  ♦ some success depending on language and circumstances, but insurers more careful about wording

♦ D&O
  ♦ How incidental breach is handled
  ♦ Approval/lack of security plans
  ♦ What is said about the cause, timing of notice, and remediation
  ♦ Compliance with new US SEC/Div. of Corporation Finance Disclosure Guidance, applicable to public companies – October 13, 2011

♦ Other lines: auto, homeowners, etc.
Issues for Excess Insurers

- Know the underlying coverage
- Follow Form
  - Understanding scope of underlying coverage
  - Knowing how primary insurer applies terms and exclusions
  - Be aware of sublimits drop downs and gaps
- Own terms → gaps in coverage?
- Reliance on primary claims handling and interpretation vs. own claims handling and interpretation
- Exhaustion/Settlements of Underlying
  - Taking over breach response and defense?
  - Agreeing/disputing exhaustion?
More Insurance Challenges:

♦ Determining the policy period
  ♦ What is the covered event and when did it take place
  ♦ Retro dates under claims made

♦ Unintended coverage
  ♦ For first party costs: the expansion of costs from data breach
    ♦ The required vs. voluntary response debate
    ♦ The expansion of what constitutes PI subject to mandatory notification
  ♦ For third party defense/indemnity
    ♦ First party costs creep under liability coverage as mitigation
    ♦ Unanticipated types of claims/damages upheld by the courts

♦ The general burden of proof on insurer to prove exclusions apply
♦ The danger of the unexpressed/unclear intent
♦ Expanding statutory, regulatory and case law: increasing obligations, liabilities, damages
♦ The Cyber Hurricane / “Cybergeddon” and Other Aggregation Issues
Insurers as Potential Targets

- Insurers are a “treasure trove for hackers” of health, personal and financial information – (NYS Dept. of Fin. Services, May 28, 2013)
- Exposures through high use of vendors
  - Typical Business Vendors
  - TPAs
    - Acting as agent of insurer
    - Access for intrusions
    - Indemnity provisions
    - Provisions as to responsibilities for breach / response
- Insurer Retention of Breach Response Vendors vs. Insured Retention/Choice
Contact Information

**Laurie A. Kamaiko**  
Steering Committee, Privacy & Data Protection Group  
Edwards Wildman Palmer LLP  
750 Lexington Avenue  
New York, New York 10022  
+1.212.912.2768  
Lkamaiko@edwardswildman.com

**Thomas J. Smedinghoff**  
Privacy & Data Protection Group  
Edwards Wildman Palmer LLP  
225 W. Wacker Drive  
Chicago, Illinois 60606  
+1.312.201.2021  
Tsmedinghoff@edwardswildman.com