Recent Developments in Data Breach Disclosure Laws

William R. Denny, Esquire
Potter Anderson & Corroon LLP
October 11, 2017
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.
We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

[Bitcoin address]

Contact Us

Check Payment

Decrypt
WannaCry ransomware hits over 150 countries exploiting leaked NSA Tool
Common Misconceptions

“Cyber crime only happens to large companies like Chase, Target and Home Depot.”

The highest rate of malware in email traffic was in organizations with 251-500 employees.
- Symantec 2017 Internet Security Threat Report

61% of all breaches occur at organizations with 250 or fewer employees
- Symantec 2014 Internet Security Threat Report

43% of all phishing attacks are targeted at organizations with 250 or fewer employees
- Symantec 2016 Internet Security Threat Report
Common Misconceptions

“My type of business isn’t a target.”

Every business is a target. Whether you operate a bank, retailer, hospital or professional service firm, everyone is at risk.

Distribution of Cyber Loss Cases:
- General Business: 44%
- Government: 15%
- Healthcare: 13%
- Education: 11%
- Banking / Finance: 7%

Source: advisen.com
Common Misconceptions

“We can self-insure against a data breach.”

Average cost of a breach is $7,350,000 (U.S. companies)

- Ponemon Institute 2017 Cost of Data Breach Study

Average cost per record is $225 (U.S. companies)

- Ponemon Institute 2017 Cost of Data Breach study
Common Misconceptions

“We don’t possess sensitive information.”

Don’t forget, cyber risk can lead to direct losses to your business as well.
- Network Business Interruption, Cyber Extortion, Bank Fraud, Fraudulent Inducement, and more
Common Misconceptions

“We outsource our network security, data management and payment transactions.”

This is a great first step toward protecting your organization, but………
Vendors are a Significant Source of Data Breaches

- Vendor Risk is one of the largest drivers of data breaches
- Most companies are not properly assessing third party risk
Delaware’s Data Breach Disclosure Law
Understanding Data Breach Disclosure Laws

- **State laws**
  - What constitutes personal information?
  - When is a notice required?
  - Who must be notified?
  - Timing of notice
  - What information must be included in notice
  - Method of delivering notice
  - Other state-specific requirements, *i.e.*, data security

- **Applicable industry-specific laws**

- **Applicable international laws**
Delaware’s Major Update

- Original law has been on the books since 2005.
- New data security obligations
- More stringent obligations for notifying affected Delaware residents
- Broader scope of what constitutes personal information
- New law goes into effect on April 14, 2018
Who is Covered by New Law?

- Every **Person** who conducts business in Delaware and who owns, licenses or maintains personal information
  - **Person**: can be an individual, governmental agency, or business, including corporation, non-profit, partnership, etc.

- Distinguish between a person that “owns or licenses” data and a person that “maintains” data for others.
  - **Owns or Licenses**: Collecting the data for your own purposes
  - **Maintains**: Managing the data for the benefit of another person, *i.e.*, a vendor hired to provide data management services.
New Data Security Requirement

- Businesses in Delaware must implement “reasonable procedures and practices” to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.”
State Data Security Laws

- At least 13 state and numerous federal laws with data security requirements

- Data security laws generally require businesses to:
  - Maintain appropriate security policies, procedures and safeguards,
  - Train employees,
  - Oversee service providers,
  - Periodically assess risks, and
  - Monitor their programs.
  - Massachusetts requires a written information security program (WISP)

- California sets a baseline for reasonable security practices: “CIS 20 Critical Security Controls.”
Massachusetts Data Security Regulations

- Companies must develop, implement and maintain a comprehensive written information security program (WISP)
  - Designate employees to maintain the WISP
  - Identify and assess reasonably foreseeable internal and external risks: data mapping
  - Develop security policies and training for employees
  - Oversee third party providers
  - Regular monitoring
  - Establish and maintain up-to-date computer security systems
  - Encryption
  - Backup tapes
Reasonable Security Practices

- Pick one standard and follow its structure and terminology.
  - NIST Framework for Improving Critical Infrastructure Cybersecurity
  - SANS Institute Risk Management Framework
  - ISO Standards 27001 through 27008
  - FAIR (Factor Analysis of Information Risk) Information Risk Management Model

- Reasonable security practices are generally understood to include policies and related training
New Breach Notification Requirements

- Key point of the law is the **duty to notify**

- What triggers the duty to notify?
  - “Determination of a **breach of security**”
  - “Determination” means having sufficient evidence to conclude that a breach of computerized data has taken place
What is a “Breach of Security”?  

- “The **unauthorized acquisition** of computerized data the compromises the **security, confidentiality, or integrity** of personal information.”

  – Some states include “**unauthorized access**” in this definition.
  – Some states expand data to include both **paper and electronic**.
What Data Must be Protected?

- **Personal Information (financial)**
  - Social Security number
  - Drivers license number
  - Credit/debit card numbers with security code or password
  - Passport number
  - Username and password or security question and answer for online account
  - Taxpayer identification number
What Data Must Be Protected?

- **Personal Information (medical)**
  - Medical history
  - Medical treatment by healthcare professional
  - Diagnosis of mental or physical condition by healthcare professional
  - DNA profile
  - Unique biometric data used for authentication purposes
What Data Must Be Protected?

- **Personal Information (insurance)**
  - Health insurance policy number
  - Subscriber identification number
  - Unique identifiers used by health insurer to identify person
Carve-outs to Personal Information

- Information lawfully made available to the general public from:
  - Federal, state, or local government records
  - Widely-distributed media
New Notification Requirements

- Person who "owns or licenses" computerized data must provide notice to Delaware residents affected by breach **within 60 days** of determination of the breach,

  - **Unless** "after an appropriate investigation," the person reasonably determines that the breach is "unlikely to result in harm," or
  - **Unless** the personal information is "encrypted" and the breach did not include access to the "encryption key" that could render the data readable, or
  - **Unless** a law enforcement agency determines that notice will impede a criminal investigation and requests that the person delay providing notice.
New Notification Requirements

- Person who “maintains” computerized data for others (i.e., a vendor) must provide notice to owner or licensee of “immediately” following determination of a breach of security.

  - NO EXCEPTION based on risk of harm analysis
  - NO EXCEPTION for law enforcement agency investigation
  - Same exception if data is “encrypted” and the breach did not include access to the “encryption key” that could render the data readable
Special Requirements and Exceptions

- Social Security numbers: one year of “credit monitoring services” at no cost to Delaware resident.
- Login credentials for an online account: clear and conspicuous notice delivered to resident online at the IP address customarily used by such resident.
- Person who maintains its own notice procedures consistent with Delaware law as part of an information security policy.
- Person who is regulated by HIPAA (health) or GLBA (financial).
Who Must Be Notified?

- Delaware residents whose personal information is breached
- Attorney General if breach involves >500 individuals
- Law enforcement NOT REQUIRED
Contents of Notice

- Delaware Attorney General will be issuing regulations prescribing the contents of notice.
- Typical notice requirements in other states:
  - General description of the incident
  - Type of information that may have been compromised
  - Steps to protect information from further unauthorized access
  - Contact information (e.g., email, 800-number)
  - Advice to affected individuals (e.g., credit reporting, review account activity)
- Other state variants
  - E.g., in Massachusetts, notice “shall not” include the number of people affected or the nature of the breach.
Notice Delivery

- Delivery methods (written, telephonic or electronic)

- Substitute notice of cost of providing notice > $75,000 or number of affected Delaware residents > 100,000
  - Electronic notice,
  - Conspicuous posting on web site, and
  - Notice to major statewide media
Developments in Other States

- 48 states, the District of Columbia, Puerto Rico, the Virgin Islands, and numerous countries with data breach laws. Numerous variations and developments:
  - Residence of affected individuals
  - Scope of “Personal information”
  - Trigger notification by “Access”
  - Inclusion of risk of harm analysis
  - Expanded list of persons receiving notice
  - Time frame for sending notice
  - Private cause of action
  - Paper v. electronic
Once an “Incident” Occurs, What Next?

- Call insurance broker/carrier
- Call attorneys to maintain privilege
- Gather members of Incident Response Team
- Determine and assign breach coordinator
- Preserve all evidence of breach and secure IT systems
  - Work with forensic specialists to contain breach
- Contact law enforcement and applicable regulators
- Determine what other actions (if any) need to be taken
Once an “Incident” Occurs, What Next?

- Determine if notices need to be sent out and to whom
  - Residence of affected individuals determines applicable notice law
  - A few states require notification of any data breach (i.e., MN)
  - Most states require notification when harm to potential victims is likely or reasonably likely (i.e., MI, OH, CA, WA)
  - Encryption or redaction may provide exception (i.e., MI, OH, DE)

- Send notices directly to affected individuals or work with mail house to effectuate
Once an “Incident” Occurs, What Next?

- Coordinate with media consultants or internal marketing for consistent messaging (press releases, FAQs)
- Provide notification to state attorneys general
- Appropriate reporting to credit card companies and credit reporting agencies
- Determine if credit monitoring will be offered
Other Privacy and Security Laws and Standards

- **Section 5(a) of the FTC Act**
  - FTC can charge defendants for violations of privacy policies under 5(a), which bars unfair and deceptive acts and practices in or affecting commerce.
    - Focus on businesses that fail to keep their security commitments or implement reasonable safeguards to protect PII.
    - FTC follows a reasonableness standard.
  - As of 2016, FTC has brought over 60 legal actions against organizations that have violated consumers’ privacy rights, or misled them by failing to maintain security for sensitive consumer information.

- **Sector-specific Laws**
  - HIPAA/HITECH (healthcare)
  - GLBA (financial services)
  - COPPA (children’s online privacy)
  - FERPA (student information)
  - TCPA (telecommunications, etc.)
Destruction/Disposal Laws

- Require physical destruction or permanently erase or otherwise render unreadable computer disks, CD, DVD, hard drives, databases, or other electronic storage tools that contain sensitive personal information
  - What do we do with old/retired hard drives, computers and copiers?
  - Can we prove it was done correctly?

- Paper copies should be shredded, cross-shredded, burned, or pulverized

- If you hire a disposal company, you must articulate requirements and monitor compliance

- Violations:
  - Knowing violations subject to criminal fines
  - Potential for civil suits
GDPR Update

  - A single set of rules across the European Union
  - Applies to any organization that retains data of EU citizens
  - Applies to any data that identifies an individual
  - Individuals have rights to access their data and request deletion.
  - Must notify local regulators within 72 hours of data loss
  - Fines apply up to €20 Million or 4% of annual global revenue

- Preparation for GDPR
  - Prepare detailed data map and identify high-risk data
  - Update policies and procedures to be GDPR-compliant
  - Some organizations must appoint a data protection officer
  - Review how you seek, record and manage consent
Proactive Measures

- Develop and implement a **Written Information Security Program (WISP)**
- Develop and implement an **Incident Response Plan**
- Review **security terms** in vendor contracts
- Ensure proper and ongoing **training** of employees
- Review **data privacy and network security**
- Explore **insurance options**
- Ensure that **management** is actively involved at all critical stages
Developing an Incident Response Plan
Cyber Incident Response Plan

- To build an IRP, companies must:
  - Identify and locate their data;
  - Evaluate the data held;
  - Reduce and eliminate unnecessary data;
  - Secure the company’s network and the data located on it; and
  - Plan for possible incidents.

- Incident Response Team (IRT) should develop the plan.
  - Include key people with authority and availability (IT, HR, legal, PR, etc.)
  - Assign distinct responsibilities with authority to act within scope of assignment.
Role of the Team

The Incident Response Team should:

- Identify necessary outside resources
- Meet at least monthly to prepare and make decisions
- Designate one person as primary point of contact
- Pre-draft important communications
- Plan what to do if electronic communication systems are unavailable
- Evaluate cyber insurance coverage
- Impose contractual obligations on vendors
- Evaluate capacity for handling a call center
- Identify criteria for notifying law enforcement and agencies
- Identify who will physically secure premises
- Identify who will isolate affected equipment
Checklist for Drafting an Effective IRP

- **The plan**
  - Assigns a specific person to lead the investigation
  - Provides a clear plan for escalating information
  - Provides a process to preserve and gather evidence
  - Incorporates legal to preserve attorney-client privilege
  - Discusses how the organization will communicate externally
  - Includes contact information for internal resources
  - Includes contact information for pre-approved external resources;
  - Is reviewed annually
  - Is tested.
Cyber Liability Insurance
Four Questions to Evaluate Cyber Insurance

1. What did you say about your business in the cyber insurance application or at renewal?

2. Do you have the right triggers?

3. What are your gaps in coverage for cyber risk and how do other policies or endorsements fix those gaps?

4. Do you have the right advocates?
The Role of the Cybersecurity Lawyer
Principal Functions of the Cybersecurity Lawyer

- Business risk analysis
- Establish key protocols
- Vendor management and contract review
- Cyber insurance review
- Conduct tabletop exercises
- Incident response
To reach us

William R. Denny
Direct dial: (302) 984-6039
wdenny@potteranderson.com

Potter Anderson & Corroon LLP
1313 North Market Street
P.O. Box 951
Wilmington, DE 19899-0951
www.potteranderson.com