Bond

Tackling the Rising Cybersecurity Threat

Albany Business Review

April 16, 2019

Tracy E. Miller
Co-Chair, Cybersecurity and Data Privacy Practice Group
tmiller@bsk.com

BOND SCHOENECK & KING

2

Highest Frequency Cyberattacks by Industry

- Financial services;
- Services companies;
- Manufacturers;
- Technology companies;
- Retailers; and
- Public sector entities.

3

Per Record Cost of Data Breach by Industry

- Health: $408
- Financial: $206
- Service Sectors: $181
- Pharmaceuticals: $174
- Technology: $170
- Education: $166

4

Leading Risks to Information Security

- Targeted attacks by hackers and cyber criminals—financial and other motives
- Employee negligence and theft
- Third parties—other providers or vendors that have your organization's data or access to information systems
- Loss or theft of mobile devices
- Vulnerabilities in information systems/devices

5

Targets for Malicious Attacks

- Employee information
- Banking information
- Credit card information
- Confidential business information
- Intellectual property
- Information system control – ransomware and viruses

6

Applicable Laws and Oversight

- GDPR
- Gramm-Leach-Bliley Act
- Tort/breach of contract cases by employees and customers
- NYS Information Security Breach and Notification Act
- Other State Notification Laws
- New York State Cybersecurity Rule
- PCI-DSS
- Federal Trade Commission Oversight

7

Overview – Building Blocks of an Effective Cybersecurity Program

- Written Policies and Procedures
- Risk Assessment
- Safeguards (Administrative, Technical, Physical)
- Workforce Policies and Training
- Effective Breach Policy
- Assigned Security Responsibility
- Third Party Agreements
- Cybersecurity Insurance

8

Risk Assessment

1. What confidential information does your organization create, receive, transmit or store?
   - Employee records
   - Financial/banking records
   - Credit card information
2. Where is the information stored/accessed/used?
   - Server(s)
   - Onsite work stations in office and at home
   - Mobile devices, e.g., laptops, phones, iPads (Mobile Devices)
3. Which employees and third parties access the information?
4. What safeguards apply to confidential information on which devices? E.g.,
   - Firewall protection
   - Password protection
   - Dual authentication
   - Remote data destruction

9

Administrative Safeguards

- Risk assessment and management.
- Assigned responsibility for security.
- Management of access to confidential information.
- Workforce security measures.
- Workforce awareness and training.
- Security incident response and reporting.
- Contingency plan to recover data in an emergency or disaster.

10

Technical and Physical Safeguards -- Examples

Technical Safeguards:

- Access control to data systems, e.g., authorization controls, automatic log off.
- Person or entity authentication to access data, e.g., passwords.
- Transmission security, e.g., encryption.
- Anti-virus/malware protection.
- Audit controls to record and examine system activity and detect breaches and malware.

Physical Safeguards:

- Secure servers.
- Access to devices.

11

Security Officer

Recommended Responsibilities

- Oversee development and implementation of security policies;
- Oversee risk assessment process and follow up;
- Oversee training for employees;
- Monitor and evaluate risks to confidential information with input from IT consultants as needed;
- Follow up promptly on reports of security concerns/breaches;
- Oversee or manage breach response;
- Conduct due diligence for transactions; and
- Prepare annual evaluation and cybersecurity plan.

12

Workforce: Safeguards for Data Access

Recommended Policy

- Access to confidential information limited to employees who need access based on job responsibility/title.
- Human resources policies and sanctions.
- System configuration to restrict access to authorization granted.
- Procedures to approve/remove access via mobile devices.
- Right to monitor access to data and use of information systems on all devices.
- Procedures to curtail access upon employee termination or for cause.

13

Mobile Devices

Recommended Policy

Employees may only use a Mobile Device, e.g. phone, laptop, iPad, whether owned by the organization or by the employee, to create, receive, store or send confidential information if:

1. Device is password protected;
2. Device can be wiped of data if lost;
3. Employees must be authorized to use a Mobile Device that accesses confidential information;
4. Employee has signed a mobile device agreement; and
5. Confidential information created, received or transmitted using a Mobile Device only if essential for a business purpose.

14

Workforce Training

Recommended Policy

- For new employees and periodically.
- Frequent, actionable reminders.
- When systems change, technology changes, or as new threats arise.
- Alerts for phishing or other scams.

15

16

BOND

Breach Policy and Response

Recommended Policy

- Written policy updated and tested.
- Identify breach response team and leadership.
- Assure coordinated response by IT and legal.
- IT expertise to analyze breach and mitigate damage.
- Counsel to oversee the investigation, assess risk, advise about notice obligations, assure attorney-client privilege protected.
- Communication plan with employees.
- Communication plan with public and individuals affected.
- Notice to individuals and enforcement agencies, as required.

17

BOND

Third Party Agreements

Among other provisions:

- Obligate the contractor to comply with all laws/regulations that apply to your organization;
- Require notice to your organization and an investigation in event of breach;
- Specify obligations in relation to any subcontractors;
- Require return or destruction of confidential information at end of underlying agreement;
- Right to terminate in the event of breach;
- Indemnification – allocate responsibility for cost of notice, remediation, etc.;
- Specify minimum necessary security practices (e.g., encryption); and
- Right to information about security practices and systems.

18

BOND

Insuring Against Cybersecurity Risk

What does your cybersecurity policy cover?

- Investigation – attorneys and consultants
- Response to regulatory enforcement
- Business interruption costs
- Notice to individuals
- Potential civil liability
- Liability to business partners for their costs
- Loss of data and/or intellectual property
- Public relations services
- Ransomware

Scope of coverage, exclusions, limits on coverage.

19

New York State Cybersecurity Rule (23 NYCRR 500)

- Applies to all entities licensed or authorized by the Department of Financial Services (DFS), including health plans
- Effective March 1, 2017, with rolling dates
- Covers all non-public information held by a Covered Entity (sensitive business information, personal/financial information about an individual, health care information)
- Highly prescriptive
- Requires annual certification of compliance to DFS by the Board of Directors or Senior Officer
- Requires all Covered Entities to develop standards for third party contractors that receive protected information.

20

NYS Cybersecurity Rule—Third Party Requirements (23 NYCRR 500)

Covered Entities must oversee cybersecurity programs of third party service providers ("Third Parties") based on a risk assessment.

Written policies and procedures that cover:

- Identification and risk assessment of Third Parties;
- Minimum Third Party cybersecurity practices;
- Due diligence to evaluate adequacy of Third Parties' cybersecurity practices;
- Periodic assessment; and
- Guidelines for contractual protections.

21

NYS Cybersecurity Rules—Third Party Requirements

Guidelines for Third Party contractual protections must cover, to the extent applicable:

- Access controls;
- Encryption in transmission and at rest;
- Notice of a cybersecurity event; and
- Representations and warranties by Third Parties in relation to cybersecurity.

22

NYS Information Security Breach and Notification Act (N.Y. Gen. Business Law §899-aa)

Who must comply?

State entities, individuals, and businesses that own, operate or maintain computerized data that includes private information.

What private information is covered?

Social security numbers, drivers license number, credit card or financial account information in combination with password/security code to the account.

What is the duty to notify?

- Notice to those whose information is disclosed without unreasonable delay or immediately to the organization that provided the data.
- Specifies methods of notice—mail, electronic, phone.
- If notice provided to any NYS residents, duty to notify the State Attorney General, Department of State, and State Police.

23

State Breach Notification Laws

All states have notification laws.

Laws differ in the definition of covered entities, covered information, required notice, and penalties.

Laws may apply based on:

- Residence of affected individuals.
- Whether the organization conducts business in the state.

In some states, the Attorney General or other state entity must be notified of a breach.

24

Payment Card Industry Data Security Standards (PCI-DSS)

- Not a law or regulation—credit card industry standards, oversight, and enforcement.
- Established by the major card brands (Visa, MC, AMEX, Discover and JCB).
- Security standards set by the "PCI Security Standards Council" designed to ensure that all entities that accept, process, store or transmit credit card information maintain a secure environment.
- Twelve basic requirements, with more specific applicable reporting standards depending on volume of credit card transactions an organization conducts annually.

25

Federal Trade Commission (FTC) Oversight

FTC oversees cybersecurity under Section 5 of FTC Act governing enforcement of unfair and deceptive commercial practices.

FTC v. Wyndham Worldwide Corporation (Third Cir. 2015)

- Affirmed FTC oversight and jurisdiction.
- Held that Wyndham had failed to use commercially reasonable safeguards as promised on its website.
- Violations of FTC standards included:
  i. Failed to encrypt stored credit card information;
  ii. Did not use industry standard password complexity;
  iii. Did not use reasonable measures to detect and prevent unauthorized access; and
  iv. Inadequate incident response.

26

Expanding Liability for a Breach—Evolving Case Law

***Dittman v. University of Pittsburgh Medical Center* (Penn. S.Ct. Nov. 2018)**

- Employee class action seeking monetary damages
- Asserted grounds—negligence/tort claim for failure to exercise reasonable care in cybersecurity practices

Held: Employee class action can move forward on tort claim.

***Sackin v. Transperfect Global* (S.D.N.Y. Oct. 2017)**

- Employee class action seeking monetary damages
- Asserted grounds--common law negligence/tort, breach of contract, unjust enrichment, violation of NY Labor Law Section 203-d
- Employer sought to dismiss for lack of standing—no cognizable injury

Held: Risk of identity theft upheld as sufficient cognizable injury.

- All grounds for suit upheld, except express contract
- Private right of action upheld under N.Y. Labor Law

27