MANAGING A CYBERSECURITY BREACH INVESTIGATION:

PRESENTATION FOR

THE ASSOCIATION OF CORPORATE COUNSEL

TODD TAYLOR, MOORE & VAN ALLEN, PLLC
RAFAEL NUNEZ, FORTALICE SOLUTIONS

May 7, 2019

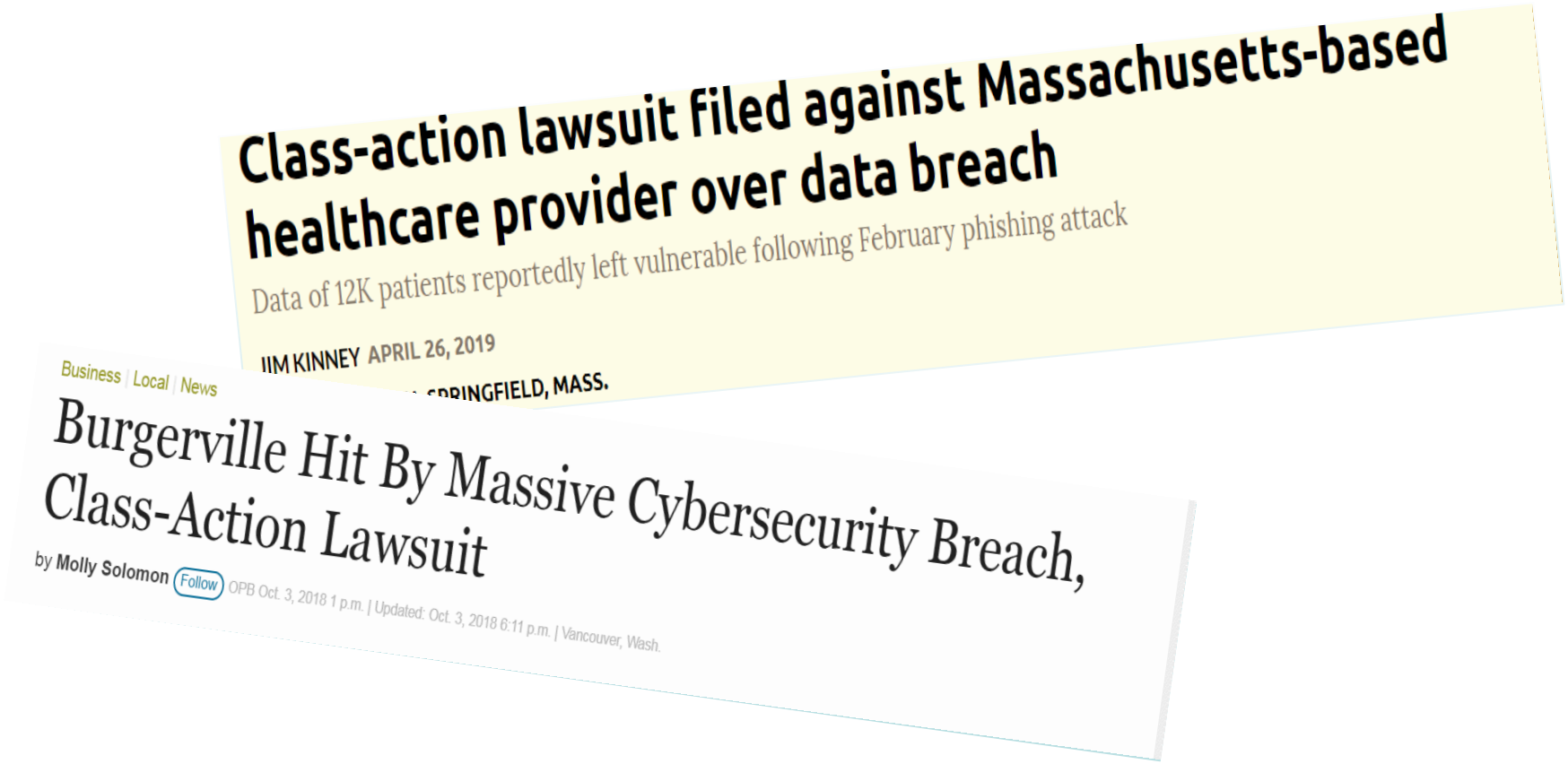
Fortalice

Cybersecurity Services

May 2019

INTRODUCTION

The Fear of Breach



Class-action lawsuit filed against Massachusetts-based healthcare provider over data breach

Data of 12K patients reportedly left vulnerable following February phishing attack

JIM KINNEY APRIL 26, 2019

SPRINGFIELD, MASS.

Business | Local | News

Burgerville Hit By Massive Cybersecurity Breach, Class-Action Lawsuit

by Molly Solomon Follow OPB Oct. 3, 2018 1 p.m. | Updated: Oct. 3, 2018 6:11 p.m. | Vancouver, Wash.

★ Evolving Threat Landscape

40% of acquiring companies engaged in a M&A transaction said they discovered a cybersecurity problem during the post-acquisition integration of the acquired company.

Healthcare data breaches cost organizations $380 per record.

Healthcare providers are 4.5x more likely to be hit with ransomware than other industries.

Ransomware accounts for 85% of all malware in healthcare.

95% of successful malware attacks are caused by spear phishing.

Most Challenging Cyber Attack Categories for Security Professionals

Mobile Devices

Data in Public Cloud

Cloud Infrastructure

User Behavior (For Example, Clicking Malicious Links in Email or Websites)

Key takeaway: Cybersecurity threats continue to morph and evolve. Companies should continue to be nimble and dynamic, in order to effectively manage threats.

Fighting the Fear

- Plan
- Implement/Test
- Investigate
- Respond
- Remediate

Incident/Event vs. Breach

- ***Event*** – any observable occurrence in a network or system.*

- ***Incident*** – a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.*

- ***Breach*** – definition varies based on law, but generally includes unauthorized access/acquisition of unencrypted personal information.

  - Under some laws, data must be in electronic or computerized form for breach to occur.
  - Some jurisdictions have risk of harm tests.

* From *NIST Special Publication 800-61, Revision 2.*

OVERVIEW OF THE LAW:
Data Security Obligations

Data Security Obligations: International and U.S. Sector Specific

GDPR – must implement ***appropriate*** technical and organizational measures to ensure a level of security ***appropriate to the risk***.

GLBA/Regulation S-P – broker/dealers, investment companies and advisers must adopt written policies with ***reasonable and appropriate*** administrative, technical, and physical safeguards for the protection of customer records and information.

NY DFS Cybersecurity Regulations – regulated entities must maintain a ***risk-based*** cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems.

GLBA/Interagency Guidelines – financial institutions must implement written information security program that includes administrative, technical, and physical safeguards ***appropriate to the size and complexity of the entity and the nature and scope of its activities***.

HIPAA Security Rule – requires covered entities to maintain ***reasonable and appropriate*** administrative, technical, and physical safeguards for protecting e-PHI.

NERC CIP Requirements – requires certain bulk power system entities to have ***risk-based*** plans and processes to safeguard critical cyber assets.

- **Key Concepts** – reasonable, appropriate and risk-based.

Data Security Obligations: Section 5 of the FTC Act

The FTC has used its authority under the Section 5 unfairness standard to pursue companies for poor security practices.

- *FTC v. Wyndham* Hotels, 799 F.3d 236 (2015) – FTC alleges Wyndham violated Section 5 by failing to maintain "***reasonable and appropriate data security***" for consumer data.

Data Security Obligations: State Data Security Laws

Currently, at least 22 states have some form of general data security requirement:

- Alabama
- Arkansas
- California
- Colorado
- Connecticut
- Delaware
- Florida
- Illinois
- Indiana
- Kansas
- Louisiana
- Maryland
- Massachusetts
- Minnesota
- Nebraska
- Nevada
- New Mexico
- Oregon
- Rhode Island
- Texas
- Utah
- Vermont

Data Security Obligations: Examples of State Data Security Laws

- **California** – must 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)***.

- **Massachusetts** – must develop, implement, and maintain a written information security program that contains ***appropriate*** administrative, technical, and physical safeguards for protection of personal information. ***201 CMR 17.03(1)***.

Data Security Obligations: Examples of Industry Security Standards

- **Payment Card Industry Data Security Standard (PCI DSS)** –
  - PCI DSS was originally adopted by Visa, MasterCard, Discover, American Express and Japan Credit Bureau.
  - PCI DSS sets forth minimum technical and operational requirements for the protection of cardholder data.
  - PCI DSS applies to all entities involved in payment card processing – including merchants.
- **ISO/IEC 27000** – series of information security standards promulgated by the International Organization for Standardization and the International Electrotechnical Commission.
- **NIST 800-53** – a set of security controls promulgated for U.S. federal information systems and their third party service providers by the National Institute of Standards and Technology.

OVERVIEW OF THE LAW:
Data Breach Notification & Disclosure

Data Breach Notification: GDPR

- GDPR requires controller "where feasible" to provide notice of personal data breach to DPA within ***72 hours*** following awareness of breach.

- If data breach is likely to result in a ***high risk to the rights of persons***, the Controller shall communicate breach to data subject "without undue delay".

- Processor shall notify Controller "without undue delay" after becoming aware of a data breach.

Data Breach Notification: GLBA/Interagency Security Guidelines

- Following an incident of unauthorized access to sensitive customer information, FI should conduct reasonable investigation.
- If FI determines that misuse of customer information has occurred or is reasonably possible, it should notify the affected customer as soon as possible.
- Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides FI with a written request for the delay.
- FI must also notify primary Federal regulator as soon as possible when FI becomes aware of an incident involving unauthorized access to or use of sensitive customer information.

Data Breach Notification: New York DFS Cybersecurity Regulations

Each covered entity shall notify DFS no later than 72 hours from a determination of:

- Cybersecurity Events impacting the covered entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or
- Cybersecurity Events that have a ***reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity***.

* Cybersecurity Event – means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an electronic information system or information stored on such information system.

Data Breach Notification: HIPAA/HITECH

- Notification – Covered entities under HIPAA/HITECH must, following the discovery of the breach of unsecured protected health information, notify the impacted individuals in writing (via first class mail, or if previously agreed to by the impacted individuals, email).

- Timing of Notice – Generally speaking, notice must be provided no later than 60 calendar days following notice of breach. However, upon request of law enforcement, notice can be delayed if the notice would impede a criminal investigation or damage national security.

- Notice to HHS – If 500 or more individuals were impacted by the breach, notice must also be promptly sent to the Secretary of HHS (if less than 500 people were impacted, notice can be sent to the Secretary within 60 days following the end of the relevant calendar year).

- Notice to Media – If more than 500 individuals in a state or jurisdiction were impacted by the breach, notice must also be given to prominent media outlets serving the state/jurisdiction.

- Notice by Business Associates & Vendors – Notification requirements also exist for business associates and certain third party service providers under HIPAA.

Data Breach Notification: State Laws

- Widespread Adoption – All 50 states have adopted some form of data breach notification laws.
- Protect "personally identifiable information" – State data breach laws generally protect name in combination with other data (*e.g.*, driver's license#, ss#, financial account numbers – sometimes in combination with passcode), if not publicly available.
- Notice Requirements – Some variation in notice requirements across the states, but notice is typically triggered when data holder reasonably believes there has been disclosure/access to NPI by an unauthorized person (often with safe harbors for encryption/no reasonably likelihood of harm).

Data Breach Notification: North Carolina

- "***Security Breach***" – an incident of unauthorized access to and acquisition of unencrypted data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer.
- Notification of a breach must be provided to all affected residents without unreasonable delay following discovery or notification of the breach.
- Must also notify without unreasonable delay the Consumer Protection Division of the NC Att'y General's Office.
- If notification is required to be given to ***more than 1,000 persons*** at one time, notification must also be given, without unreasonable delay, to consumer reporting agencies.

Data Breach Notification: Key Takeaways

- Know the triggers for notification (may vary based on data/jurisdiction).
- Know the persons/entities/authorities to be notified.
- Pay attention to timing requirements.
- Comply with notice content requirements of applicable jurisdiction.
- Service providers may have contractual and statutory notice requirements.
- Don’t forget potential law enforcement notification delays.

Data Breach Disclosure:
SEC Release Nos. 33-10459; 34-82746

- Based on materiality, cybersecurity incidents may require disclosure in public companies' SEC required filings.
- Public companies should adopt comprehensive policies related to cybersecurity, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity incidents.
- Information about cybersecurity incidents may be MNPI, and corporate insiders would violate antifraud requirements if they trade the company's securities while in possession of that MNPI.

OVERVIEW OF THE LAW:
Potential Liability

Potential Liability: GDPR

- Administrative fines for violations of GDPR data security and notification provisions can equal up to the greater of:
  - €10 million; or
  - 2% of the worldwide "turnover" (*i.e.*, revenue) of an "undertaking" for the preceding financial year.
- Private causes of action can be asserted.

Potential Liability: CCPA

- CA Atty. Gen. can bring civil enforcement actions for violations of CCPA and obtain fines of up to $2,500.00 for each violation or up to $7,500.00 for intentional violations.

- Private causes of action can be asserted for data breaches resulting from failure to implement and maintain reasonable security procedures.

- Plaintiffs can obtain greater of statutory damages (*i.e.*, $150.00 to $750.00 per consumer per incident) or actual damages.

Potential Liability:
Examples of Other Sources of Liability

- Fines imposed by regulatory agencies (*e.g.*, FTC, CFPB, State AGs).
- Liability under UDAP laws.
- Contract breach liability.
- State tort law liability.
- PCI DSS fines.

Potential Liability: Select Cases

- **Target** – data breach impacting 41 million consumer card holders.
  - **Consumer Class Action Settlement** – $10 million settlement (up to $10K for each class member), plus attorney's fees of up to $6.75 million.
  - **Card Issuer Settlement** – $39 million settlement (including sums paid into MasterCard remediation fund), plus attorneys' fees of $17.8 million.
  - **Visa Settlement** – $67 million settlement.
  - **State Settlement** – $18.5 million paid to 47 states.

- **Yahoo** – data breaches over two years impacting 3 billion users.
  - **Shareholder Derivative Litigation Settlement** – $29 million settlement, plus $10.6 million in attorneys' fees.
  - **Shareholder Class Action Settlement** – $80 million, plus $14 million in attorneys' fees.
  - **Consumer Class Action Settlement** – $117.5 million (subject to approval).
  - **SEC Fine** – $35 million fine for failing to disclose data breach.
  - **UK ICO** – £250,000.00
  - **Verizon Acquisition** – $350 million purchase price reduction.

Potential Liability: 2018 Ponemon Study

- Average U.S. data breach per capita cost = $233.
- Average total cost of data breach in U.S. = $7.91 million.
- The faster a data breach is identified, the lower the cost of the breach.
- An incident response team can reduce costs by as much as $14 per record.
- The average costs of data breach notification in the U.S. were $740,000.
- The average costs associated with post-data breach response in the United States were $1.76 million.

PREPARING FOR A DATA INCIDENT

Preparing for a Data Incident: Data & System Inventory

- What categories of data does your organization maintain (*e.g.*, consumer, customer, employee, business proprietary)?

- Who has access to your organization's data (*e.g.*, employees, contractors, vendors)?

- Where is your organization's data maintained (*e.g.*, on premise, co-location facility, cloud).

Preparing for a Data Incident: Develop an Information Security Program

- Involve key stakeholders – NOT JUST THE LAWYERS.
- Review applicable legal and regulatory requirements.
- Build program based on nature of your business.
- Get Board/Sr. Management review and approval.

Preparing for a Data Incident: Develop an Incident Response Plan

- Key component of an Information Security Program.

- Determine if laws applicable to your business require certain items to be addressed.

Objective of IRP

"The primary objective of an incident response plan is to respond to incidents before they become a major setback."

Incident Response Plan - Development

1. Prepare

2. Assemble Response Team

3. Outline Response Requirements and Resolution Times

4. Establish a Disaster Recovery Strategy

5. Fire Drill

6. Plan for Debriefing

Preparing for a Data Incident: Validating Programs and Plans

- Train personnel on Information Security Program and Incident Response Plan.
- Ensure key service providers have adequate programs and plans.
- Review and audit Information Security Program:
  - engage third parties to conduct vulnerability/penetration tests;
  - engage in SOC 2/Type 2 reporting or similar audit process; and
  - promptly remediate deficiencies based on risk.
- Undertake tabletop exercises.

★ Prepare

- What Constitutes and Incident?
- Critical Services and Applications to Maintain Operations?
- What data exists and where is it stored?
  - Value to Business?
  - Value to Intruder?
- Conduct an Assessment. (Be Honest)

★ Build a Response Team

- Computer Security Incident Response Team (CSIRT)
- Key People to Mitigate the Immediate Issues Concerning a Data Breach.
- Technical Aspects of Incident Resolution and Communication.
- Communicates with Stakeholders Within the Organization, and External Groups (Press, Legal Counsel, Affected Customers, and Law Enforcement).

★ Outline Response Requirements and Resolution Times

- What Needs to be Contained? Short Term / Long Term.
- How Long Can You Afford to be Out of Commission?
- Quick Response Guides are Excellent.

★ Run a Fire Drill

- Conduct Tabletop Exercises
- Treat as Real-World Incident
- Utilize Relevant Injects
- Cross-Functional Participation is Key
- Document Findings and Ideas

Preparing for a Data Incident: Cyber/Data Breach Insurance

Cyber/Data Breach Insurance can include coverage for:

- third party claims (including, in some cases regulatory and PCI fines);
- initial forensic response;
- attorneys' fees;
- repair of network damages;
- notification of breach victims;
- lost revenues and business interruption;
- cyber extortion; and
- reputational damages.

RESPONDING TO A DATA INCIDENT

IT'S HERE!

Responding to a Data Incident: The Initial Steps

- Follow the Incident Response Plan.
- Involve appropriate stakeholders (*e.g.*, committee of members from IT, Info Sec, Legal, Finance, Compliance/Risk, PR).

Responding to a Data Incident: Engage Third Party Experts

Depending on the severity of the incident, the organization should consider:

- Contacting insurance carrier.
- Engaging external legal resources:
  - can manage the investigation under privilege; and
  - can assess and assist in mitigating liability to third parties.
- Engaging reputable forensic investigation firm:
  - can assist in preserving evidence;
  - can assist in determining what happened; and
  - can propose remediation steps.
- Engaging public relations firm.

Responding to a Data Incident: Investigate the Incident

- IT/forensic firm directed by lawyers, should investigate.
- Reasonable period of time can be taken to investigate incident.
- Contact law enforcement as and if necessary.
- Determine nature of incident and whether “breach” occurred.

Responding to a Data Incident: Notification and Disclosure

Based on severity and nature of incident, the organization should:

- Provide all legal/regulatory/contractually required notices.
  - Ensure notifications are made within appropriate time periods.
  - Ensure that not only impacted individuals are notified but also any required governmental authorities or other entities (*e.g.*, contract counterparties, CRAs, card processors).
  - Ensure notifications have all required content.
- Determine whether incident needs to be disclosed in public filings (if the organization is a public company).

REMEDIATING A DATA INCIDENT

★ Disaster Recovery Strategy

"When all else fails, plan for disaster recovery"

- Process of Restoring and Returning Affected Systems, Devices and Data.
- Reliable Backups and Disaster Recovery.
- Best Case – You'll Never Use It.

Remediating a Data Incident: Customer Concerns & Security Issues

- Provide legally required credit monitoring (*e.g.*, California/Connecticut).

- Consider providing optional credit monitoring and otherwise making impacted individuals whole (if reasonable and appropriate).

- Promptly remediate any security deficiencies identified during course of incident.

★ Plan for Debriefing

- Dealing with Aftermath and Areas of Improvement.
- Efficiency in Filling out Report.
- Gap analysis.
- Post Incident Activities.

Contact Information

Todd Taylor
Member
toddtaylor@mvalaw.com

Rafael Nunez
Director, Retained Services
rnunez@fortalicesolutions.com

QUESTIONS