Mika Meyers PLC
Attorneys at Law

Michigan Cyber Security Conference
October 19, 2017

Don’t Wait for the Breach to Plan Your Reaction

Security Breaches: WHEN, not if!

- Everyone will eventually be affected by a cybersecurity breach.
- Even best efforts at protecting information may not be enough.

What is a “Security Breach”?

- The unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality or integrity of personal information.
- A few states require notification of acquisition of personal information from paper records in addition to electronic records.

Breaches of Data and Information

- Physical security breach.
  - Lost device, lost paperwork, other mishandling.
  - Burglary/Robbery.
- Electronic breach.
  - Hacking.
  - Phishing.

This Presentation is Not About. . .

- Analysis of specific security tools
- Discussion regarding specific threats

This Presentation **is** About. . .

- How to reduce your potential liability both ***in advance*** of a breach and ***after*** *a breach.*
- How entities are expected to respond to a breach.
- How individuals should respond to a breach.

Who needs to be concerned?

- Owners/Licensees of Personal and Confidential Information
  - Individuals
  - Businesses
- Businesses collecting, storing or using confidential information
  - Service providers
  - Employers

Protection of Data Privacy

- What must be done
- What should be done
- Why every business should have:
  - A security and data protection program,
  - A data breach response plan, and
  - A privacy policy and security policy.

What must businesses do to protect confidential information?

- No single comprehensive federal privacy or data security law
- Sector-specific federal privacy and data protection laws.
- State laws - most states require that “reasonable information security measures” be used.
  - Protect information from unauthorized access, destruction, use, modification and disclosure.
  - Use reasonable records retention/destruction procedures.

What must businesses do to protect information (cont'd)?

- Industry guidelines
- Contractual requirements
- International laws

What are “Reasonable Information Security Measures”?

- Secure your network
  - E.g., user authentication mechanisms, restrictions on use, firewalls, anti-virus software, intrusion detection systems
  - Different technologies may be appropriate for different data
- Educate Employees regarding scams and risks
  - Implement policies and rules regarding employee use of technology
  - Require confidentiality agreements
- Contractually require vendors to use reasonable security procedures
- Encryption

Penalties for failing to comply with security requirements (in the U.S.)

- Federal agencies and states enforce privacy and security.
- Fines.
- Private rights of action.

What should individuals do to protect their confidential information?

Reasonable information security measures!

What should businesses do to protect confidential information?

- Proactively and mindfully create cyber security program.
  - Assess risks.
  - Address breach avoidance through implementation of reasonable procedures and policies to protect sensitive information.
  - Plan for data loss with business continuity plan (e.g., back up data).
  - Develop breach response plan.
- Monitor, update, evolve to keep pace with changing circumstances.
- Consider cyber security insurance that protects against security incidents and covers expenses of response.

Why bother with a Program, Plan, and Policy?

- Several states' statutes specify that an entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information shall be deemed in compliance with the statute if its notifications are consistent with its policies.

Encryption Safe Harbor

- Most breach notification statues do not require notification if disclosed personal information is encrypted, and encryption key was not part of breach.

When there is a breach:
Immediate Action Steps - Containment and Continuity

- Identify and isolate affected programs, processes and systems.
- Engage response team (attorney, insurer, IT professionals).
- Preserve evidence.

When there is a breach:
Continuing Actions – Information Gathering

- Document and describe incident related events.
  - Who, what, where, when, why, how.
- Identify all data affected by the incident, and how it was affected.
  - E.g., what kind of data, was data accessed, lost, etc.

When there is a breach:

Continuing Actions – Determine Response to Breach

- Determine whether breach notification to third parties is required by:
  - Applicable law;
  - Contractual requirement; or
  - Company policy.
- Consider public relations.

What is “Personal Information”?

- Definition of “personal information” varies by state.
- Generally:
  - Individual’s first name or initial and last name plus one of the following.
    - SSN.
    - Drivers license number or state issued ID number.
    - Account number, credit or debit card number combined with security/access code PIN or password needed to access account.
  - Doesn’t include publicly available information.

“Personal Information” Can Also Mean

- Medical information.
- Alien registration numbers, government passport numbers.
- Username/email address in combination with password/security question + answer that would permit access to online account.
- Unique biometric data (fingerprint, retina image, etc.).

Statutory Requirements for Breach Response

- 48 US states require particular actions in response to security breach of personal information.
- Notice of breach often required to be sent to affected individuals, data owners, regulators, consumer reporting agencies.
- Statutes vary regarding:
  - Content of notice.
  - Time for delivery.
  - Delivery method.

What Triggers Notification?

- Access to personal information.
- Risk of harm to individual.
  - Reasonable likelihood of harm.
  - No substantial risk of identity theft or fraud.
  - Michigan: not likely to cause substantial loss or injury to, or result in identity theft with respect to, one or more residents.

Who Must Deliver Notice?

- State law varies, but typically any person, agency or entity that owns or licenses personal information.
- Entities maintaining personal information but which do not own or license the use of information may have different reporting/notice obligations.

Who Must Be Notified?

- Owner of the personal information.
  - State residents (individuals).
- Entity licensing or owning data.
- Third parties.
  - Some states (e.g. Connecticut, Montana) require notice to state attorney general if residents are notified.
  - Other states only require notice to state government agencies when a large number of state residents are affected.
  - Some states also require notification to consumer reporting agency.

How Can Notice Be Delivered?

- Written notice (snail mail) to postal address in entity's records.
- Electronic notice (under certain circumstances, in some states).
- Telephone notice (under certain circumstances, in some states).
- Substitute notice.
  - Email.
  - Posting on website.
  - Notification to statewide media.

Deadline for Delivering Notice

- Most expedient time possible.
- Without unreasonable delay.
- Some states provide a specific deadline, for example.
  - 30 days after discovery of breach.
  - 45 days after discovery of breach.
  - Licensing of CT Insurance Department must notify department five days after discovery of breach.

What Must the Notice Say?

- Depends on state law.
- Most states have similar requirements regarding content.
- Some states have very specific and different requirements (e.g. California).

Contents of Breach Notice Regarding the Incident

- Date of the breach.
- Nature of the breach.
- Steps being taken to protect data from further breaches.
- Type of information affected by the breach.

Contact Information in the Breach Notice

- Contact information from the affected entity that can be used to inquire about the security or the breach.
- Toll free numbers and addresses for consumer reporting agencies.
- Toll free number and address and website address from FTC.

Other Items in the Breach Notice

- Reminder of the need to be vigilant for incidents of fraud and identify theft.
- Statement that the individual can obtain information about fraud alerts and security freezes.
- Encourage victim to review account statements and monitor free credit reports.

How to Make this Easier

- Address inventory and process in advance in an information security policy and response plan.
- Know and understand what data you have.
- Encryption!

Incident Response Plan

- List procedures to guide employees on what to do in the event of a breach.
- Identify responsible parties and external team players in advance.
- PRACTICE.
- Update as needed.

Data Breach Response Checklist

- Make one, or get one. (Email me and I'm happy to share mine with you.)
- Look at the checklist **before** a breach to identify your response team, data in your control, relevant jurisdictions that may have laws with which you need to comply.
- Update the checklist regularly.
- Pull out the checklist in the event of a breach to start organizing **and** documenting your response.

Cyber Insurance

- Some risks related to cyber liability are excluded from traditional general liability policies.
- Cyber insurance may include coverage against losses such as data destruction, hacking, theft, DNS attacks.
- May cover liability for breach, cost of restoring operations, costs for consumer notification, etc.

Equifax

- The following information has been offered by the Michigan attorney general regarding the Equifax breach: http://www.michigan.gov/documents/ag/What_You_Need_to_Know_About_the_Equifax_Breach_accessbile_600814_7.pdf
- The Michigan AG has joined with more than 40 other state attorneys general in investigating the breach
- Ensure that status has not changed and to take appropriate steps to protect your information if it has. You can check your status here: https://www.equifaxsecurity2017.com/

Equifax

- For general consumer questions or complaints, you may also reach the Attorney General's Consumer Protection Division at:

  Consumer Protection Division

  P.O. Box 30213

  Lansing, MI 48909

  (517) 373-1140

  Fax: (517) 241-3771

  Toll Free: (877) 765-8388

Questions?

Jennifer Puplava

(616) 632-8050

jpuplava@mikameyers.com