SMALL BUSINESS BIG THREAT

Small Business, Big Threat

What to do if your business is the victim of a data or security breach?

Introduction

The following information is intended to help you decide how to start preparing for and some of the steps you will want to take in the event security breach regarding certain types of data and information. As it is not possible to cover all scenarios and circumstances, there may be other considerations or steps that you will want to follow which are not included in this review.

Mandiant's 2014 threat report – cites an average of 243 days to discover a breach. Given the near-certainty that some form of an attack or data breach will happen in your organization, likely via mobile devices, it makes sense to consider scenarios and plan for them prior to the incident occurring. A data breach plan lays out the key steps and the key personnel to involve.

For assistance in better understanding your obligations and tailoring a security breach reaction plan for your company it is therefore highly recommended that you consult with your technology and\or legal partners.

Know the Law

Michigan has enacted laws requiring certain actions are taken and that individuals be notified when a security breach compromises personal information. If you believe your security has been breached you should review and understand any obligation you may have under **Mich. Comp. Laws §§ 445.63, 445.72.**

In addition to the state laws described above, **federal law** may require notice for certain types of data breaches.

AMERICA'S SBDC IOWA
POWERED BY SBA U.S. Small Business Administration
IOWA STATE UNIVERSITY COLLEGE OF BUSINESS

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation

Small Business, Big Threat

Financial institutions subject to the federal Gramm-Leach-Bliley Act (15 U.S.C. §§6801-6810) must adopt procedures to safeguard customer data and notify customers when there has been unauthorized access to customer data if the financial institution determines that customer data has been or is likely to be misused. Guidelines on when customers of a financial institution should be notified about a data breach are published by the FDIC.

Data breaches involving **medical information or other related personal health information** may also prompt the requirement to notify certain parties. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act. It's important to remember that even if you are not a medical provider yourself. These rules may apply to you if you work closely with any association which is or which services a Health provider other related organization.

For more information from HHS about HIPAA breaches go here.

The HITECH Act also requires the Federal Trade Commission (FTC) to adopt data breach rules that apply to web-based vendors of electronic personal health information as well as the vendors' service providers. Read the FTC's breach notification rule here.

It has become a "**best practice**", if not common practice for companies, educational institutions, and government agencies to notify their customers and employees whether or not the breach they've experienced requires that they provide notice to their customers and/or employees. One example is breaches in which customers' names and email addresses may have been compromised. Even if the information exposed in these breaches would not likely lead to financial identity theft if obtained by criminals, many companies have elected to notify their customers anyway.

Before A Breach Occurs

First and foremost, if you do not already have both an action plan and response team defined, do so now. Understanding your responsibility and planning ahead will greatly assist you in the event of a suspected security breach. The guidelines below will help you consider all the things your plan should contain.

Small Business, Big Threat

First, know your data.

- Where it is (*"in the cloud" vs. on the server in the back*).
- How it flows (*only within your physical office vs. wherever your sales team accesses it via their mobile device).*
- Who has access to the data? (*does everyone have equal access or is access granted based on an individual's job title?*).
- Is your data encrypted – in transit and/or at rest?
- Is all data considered to be sensitive, or only specific data sets?

Second, how is data monitored?

- Is there a log that records each and every person and/or system that touches (*or attempts to touch*) sensitive data? Data breach researchers recommend that all businesses implement a security information and event-monitoring program to aid with discovering malicious activity and possibly mitigate the attack, assist with legal prosecution, or provide details/forensics to an insurance company if you need to make a claim.

Third, understand your data.

- Why is it valuable?
- Who would want to steal it? This should lead to an understanding of what type of attacker may be interested in committing a data breach. One suggestion would be to contact law enforcement to see if similar companies have had breaches. If so, try to learn as much about the breach as possible.
- What was taken?
    - When was the data breach discovered?
- Ask the usual questions – why, how, when, where, who - in order that you may learn from that unfortunate company's experience and be prepared in advance.

People to Involve

- Know who you'll call for help
- Establish an incident response team
- Provide regular training for employees; keeping an outside team—including forensic experts, privacy counsel and communications firms—close by

Process to Follow

- Know what data you are protecting and where it is stored
- Go through hypothetical breach scenarios with a response team

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation

- Know which employees have access to which applications and learn what the reporting obligations may be in case of a breach

Technology You'll Need

- Enable network logging, and be sure it's sufficiently detailed
- Back up servers and be sure backups are under control
- Enforce records management, and destroy old data
- Implement full-disk encryption on laptops
- Implement increased security measures, such as password standards
- Implement DLP to monitor the perimeter
- Effectively manage security integration from acquisitions

During A Breach

Above all, don't panic. A security breach does not necessarily mean that you or your customers will become a victim of identity theft. Whether or not it is likely your customers will be compromised as a result of the breach communication with them may be essential.

Once a data breach is discovered, as part of your 'incident response', consult your company's back-up and recovery plan. If back-ups are not routinely done, out-of-date data may result in losing everything in an instant; therefore it is critical to have frequent and regular back-ups of company data.

If you do decide or need to contact your customers make sure they know you will take care of them. Resist finger pointing and playing the blame game. Let your customers know you take the breach seriously and that you are reacting to it. Follow through on what you promise to do. Living by your commitments is essential so that you do not lose your customers trust.
The following information will help you identify ways to reduce your risk and exposure regarding identity theft.

If you do decide or need to contact your customers make sure they know you will take care of them. Resist finger pointing and playing the blame game. Let your customers know you take the breach seriously and that you are reacting to it. Follow through on what you promise to do. Living by your commitments is essential so that you do not lose your customers trust.

The following information will help you identify ways to reduce your risk and exposure regarding identity theft.

People to Involve

- It's important to keep the group of people who are "in the know" small
- Engage forensic experts, a communications team and privacy counsel from the beginning
- Effectively manage incident response project management

- Anticipate threats internally and externally
- Consider the impact of third parties

Process to Follow

- Act immediately to remediate vulnerabilities
- Don't reach out to the public too soon
- Cast a wide data-mining net
- Document actions taken to share with regulators later
- Update investigative team
- Do not communicate preliminary numbers
- Consider each finding's business impact

Technology You'll Need

- Take live memory dumps before shutting down servers
- Insist on full forensic images of servers and laptops
- Pull network logs immediately, and increase log capacity
- Pull oldest available backups
- Rest passwords quickly
- Be careful with evidence handling

Keep in mind, there is an increase in ransomware* attacks by hackers. It is also important to note that the compromise of ***Personally Identifiable Information**** (PII) may result in civil litigation against your firm by your state's attorney general, as well as other legal actions.

Ransomware *– a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom thru online payment methods in order to grant access to their systems, or to get their data back. Some ransomware encrypts files (called Cryptolocker).*

***Personally Identifiable Information (PII)** – any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data. In other words, information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PII includes Social Security Numbers, driver's license numbers, medical data, and other information that is not considered to be "public".*

After A Breach

Don't assume it's over until it's over. Make sure the breach and any associated risk have been mitigated.

Step 1: Review Your Legal and Ethical Obligations

Data breaches are complex; they typically involve a number of federal and state laws that will dictate how and when to notify affected customers, state officials (Attorney General, State Commissions, regulators), etc. It is suggested that all business owners review and understand what is expected of your business – preferably with the advice of an attorney that is well versed in data breach law since some of these laws and/or regulations may impose strict deadlines for reporting a breach. At the same time, fulfilling the ethical obligations to your business' customers, vendors and employees, may require you to exceed the letter of the law.

Step 2: Don't Panic…and Don't Rush Your Response

A reliable resource is the Ponemon Institute, and this organization suggests that businesses act as quickly as possible to respond to a data breach and notify their customers. HOWEVER, do not rush to meet with the media until you have received approval from law enforcement. Another important reason NOT to rush to share data breach information is that "quick responders" actually end up paying more per breached record than companies that wait a bit longer to execute their response strategies and gather as many facts as possible. The bottom line of this vicious cycle: Companies end up spending as much time correcting the impact of their own misinformation about their required actions in a breach situation as they do in dealing with the impact of the original breach.

Step 3: Perform an Analysis, and Act on Your Results

Even though it has been proven that breaches typically involve failure to apply technology properly, a business must still create and execute cyber-security initiatives for mobile devices, software, hardware, and firmware to the best of your ability; this is where utilizing the services of a professional provide significant value.

One problem that is impossible to prevent is the 'lost or stolen laptop' problem — we all understand that it's going to happen at some point. But your business can impose strict data encryption requirements on these systems or require employees to store sensitive data on your network instead of on the device itself, accessing it only through a VPN (*Virtual Private Network*)* connection. Businesses can also combine these technology tools with policy and training measures that hold employees responsible for violating data security policies.

****virtual private network** – a method of employing encryption to provide secure access to a remote computer over the Internet. It enables users to send and receive data across shared or public networks as if their devices were directly connected to the private network, and thus are benefiting from the functionality, security and management policies of the private network.*

A data breach analysis may result in additional ways to improve your business' use of technology. Network and endpoint security, anti-malware tools, anti-phishing tools and policies, and other solutions can work together to protect you, your employees, your customers, vendors and your business.

Another suggestion is to hire an outside consultant to perform a post-breach security audit of your company's systems and data handling procedures. You may think you know why a breach happened, but an objective, outside analysis might turn up a very different set of answers to that vital question.

Step 4: Keep Your Customers and Employees in the Loop

Technology can play a vital role in helping your company avoid future data breaches. Information regarding new policies and procedures can be shared with employees and customers, but deluging your audience with technical details about your security procedures — that's as pointless (and dangerous) as it sounds.

People to Involve

- Use the breach exposure to promote the enhancement of the security program to your board
- Revisit data governance structure, including security, legal and risk management
- Deliver your employees and customers a transparent and consistent message
- Use the opportunity to roll out privacy training

Process to Follow

- Use the opportunity to expand privacy and security programs
- Document lessons learned
- Do not over communicate or revise numbers
- Anticipate long-term regulatory scrutiny
- Use the opportunity to build privacy and security into new initiatives
- Build a playbook

Technology You'll Need

- Develop a remediation plan with technology enhancements
- Test remediation actions
- Consider company wide improvements
- Preserve investigative evidence
- Update encryption, external media, USB and e-mail policies
- Review cloud and third-party technology providers' preparedness

Mobile device-specific breaches (including fraudulent texts and other mobile issues)

- Each wireless carrier has a fraud text number and fraud email address to which suspected content should be forwarded. Check with your wireless carrier in advance to make sure you have them on file. If you receive a text message you suspect as being fraudulent or a security risk in any way – DO NOT OPEN IT – immediately forward it to the text number

provided by your carrier. Do the same with an email you receive and have concerns about; again – DO NOT OPEN IT – instead, immediately forward the suspect email to the fraud-reporting email provided by your carrier

- If you suspect that an App you have downloaded contains a virus, malware, or is malicious in some other way, notify the app store from which it was downloaded and have a tech security professional assess its impact on your mobile device.

Connected Vehicle Breach

- Don't freak out. Calmly step back and assess the situation before taking any action. Be sure you can clearly explain the situation to those you may need to notify such as: law enforcement, the manufacturer, the dealer, or your repair shop.

- If it appears your car has been hacked or tampered with, don't drive the car until it has been assessed and any issues have been resolved.

- If you think there is an issue with a connected vehicle system and it is appearing to have been hacked, check with the manufacturer to determine if it may be an issue for which a recall may have been initiated, and may not necessarily be a hacking issue.

• As soon as possible update your vehicle systems with the latest software release and going forward implement all updates promptly

Security Breach Review - The Do's and Don'ts

Do –

✓ Have a written breach response plan ready
✓ Test your plan before a breach happens
✓ Identify a breach response team and make sure people know what role they will play when a breach happens
✓ Have a communications plan regarding the breach
✓ Know what regulations, statutes and contracts cover your post-breach obligations
✓ When a breach happens, pull out the stops to prevent further exposure of data
✓ Find out what happened as soon as possible and preserve the evidence
✓ Contact your insurance carrier and seek legal advice regarding whether the breach triggers notifications requirements and whether those notification requirements apply to your company
✓ Involve technology and legal experts as needed
✓ Have draft model notices ready to be customized depending on the facts
✓ Contact law enforcement, credit reporting agencies, and keep regulators informed where required by law and where appropriate

Don't –

× Delay in providing notices when legal counsel determines they are required or advisable – the time deadlines are strict
× Communicate with the public about the breach until you know the fundamental facts
× Ignore your important business customers and partners – keep them informed
× Necessarily accede to every demand from a business customer and partner –weigh demands carefully in light of your total response plan
× Skimp in providing help to consumers – their goodwill could forestall legal difficulties
× Forget to update your post-breach response plan regularly

IMPORTANT NOTE:

The following information is intended to help you decide how to start preparing to secure your business against a cyber-attack, and some of the steps you may want to take in the event security breach regarding certain types of data and information. As it is not possible to cover all scenarios and circumstances, there may be other considerations or steps that you will want to follow which are not included in this review. For assistance in better understanding your obligations and tailoring a security breach reaction plan for your company it is therefore highly recommended that you consult with your technology and\or legal partners.