WOLF
& COMPANY, P.C.

Belmont Savings Bank

Are there “Hackers at the gate?”

About Wolf & Company, P.C.

- Established in 1911
- Offers Audit, Tax and Risk Management Services
- Offices located in:
  - Boston, MA
  - Springfield, MA
  - Albany, NY
- Over 170 professionals
- Committed to industry excellence

As a leading regional firm founded in 1911, we provide our clients with specialized industry expertise and outstanding service.

Our Expertise

- Closely Held and Family Businesses
- Financial Institutions
- Healthcare
- High Net Worth Individuals
- Investment Advisors and Partnerships
- Pension Plans
- Technology Companies

IT Assurance Services

Wolf's IT Assurance professionals have detailed knowledge of business operations and technologies.

- IT Audit
- Information Privacy Review
- Application Security Review
- Network Vulnerability Assessments
- Social Engineering Assessment
- Business Continuity Planning (BCP)
- Incident Response Planning (IRP)
- Policy & Procedure Development
- Internal IT Audit Support (SOX 404)
- SSAE16 & SysTrust Assurance

Agenda

- The state of data security
- Why is information security important?
- How hackers get in
- Massachusetts Privacy Law
- How to protect your company

WOLF
& COMPANY, P.C.

“As we know,
There are known knowns.
There are things we know we know.
We also know
There are known unknowns.
That is to say
We know there are some things
We do not know.
But there are also unknown unknowns,
The ones we don't know
We don't know.”

— Donald Rumsfeld, Feb. 12, 2002,
Department of Defense news briefing

Stolen laptop and disks…

Safe stolen from Dayton chiropractic office

By **Dissent**, November 27, 2012 9:23 pm

NewsTalkRadioWHIO reports:

> A chiropractic office was broken into early Monday morning and reportedly had a safe and computer stolen.
>
> The break in occurred at about 1:30 a.m. at **Long Chiropractic**, located at 4978 Northcutt Pl., according to a Dayton Police incident report.
>
> Thieves broke out a window on the south side of the building and got away with the safe full of computer disks and a laptop computer.

Documents in the Dumpster…

Sensitive data found in dumpster reveals SSNs and health info

A large number of medical documents and files containing private information were found in a dumpster outside of an office complex in Hiram, Ga.

How many victims? The number of people affected has not been disclosed.

What type of personal information? Social Security numbers, addresses, dates of birth, bank account information and private health information.

What happened? After receiving an anonymous tip, a local news reporter discovered the personal information in a dumpster just outside of an office complex.

What was the response? The Hiram Police Department contacted an FBI field office in Rome, Ga. An agent was sent to investigate the matter.

Details: Ross Cavitt, a Channel 2 Action News reporter, was given a tip from an anonymous caller about the disposed information. After discovering the dumpster filled with the private data, he contacted the Hiram Police Department. According to Cavitt, the documents found came from an orthopedic practice, as well as the office of Family Intervention Services in a nearby complex. Both businesses had recently moved out.

http://www.scmagazine.com/sensitive-data-found-in-dumpster-reveals-ssns-and-health-info/article/283478/

Accidental Disclosure…

Massachusetts Police Department Suffers Data Breach

Police log contained personal information for 100-plus

Wednesday, January 30, 2013

The police department in Littleton, Massachusetts, recently suffered a data breach that exposed more than a hundred people as a result of its activity log being posted online as normal, but with a wealth of personal information attached.

The department regularly publishes a normal police log on its site, but a "personal error" exposed the names, dates of birth, addresses and Social Security numbers for anyone who were pulled over, arrested, involved in a car accident, reported a crime, or required medical attention as a result of a police call in the town between January 7 and 13, according to a report from the Lowell Sun. The breach was caused by the person uploading the information using the wrong menu to do so.

http://idt911.com/en/sitecore/content/GlobalElements/KnowledgeCenter/NewsAlertItems/374908.aspx

State Breach…

Massachusetts Data Breach Exposes 139,000 Records

By Stefanie Hoffman, CRN

Jul. 07, 2010 6:09 PM EST

The Massachusetts Secretary of State's office became the latest data breach victim when an employee accidentally released confidential information of 139,000 state-registered investment advisers to a business publication.

The breach occurred when personal information of tens of thousands of investment professionals contained on a CD-ROM was sent to *IA Week*, an investment industry publication, in response to a request for public information. *IA Week* had issued an information request of the office's Securities Division for a list of registered investment companies, but was instead sent a list of investment professionals.

A new employee was culpable for the breach by failing to delete the investment advisers' Social Security numbers and other private information, which is normally withheld for such requests.

Altogether, the exposed information included the investors' names, Social Security numbers, birth dates and locations, in addition to height, weight and hair and eye color.

RECENT ARTICLES

Security Goes Platinum: Conference 2011

RSA Conference 2011 had a it's impossible to see and do i the nation's largest informatio

25 More Head-Turning S At RSA Conference 2011

Security vendors rolled out th offerings at RSA Conference caught our attention on the sh

RSA At The Movies: Secu Of Hollywood Cybercrim

From The Net to Live Free Or professionals at RSA Confer films to see if these Hollywoo happen.

More Slide Shows

http://www.crn.com/news/security/225702618/massachusetts-data-breach-exposes-139-000-records.htm;jsessionid=aYSJ2zVZobh0B7pKEdkmBQ**.ecappj01

Why is Information Security Important?

- Need to provide confidentiality, integrity, and availability of information assets
- To maintain trust, image, credibility:
  people entrust us with their personal information so that we can help protect them, and build a solid foundation for their financial security
- Security incidents cost $$$$
- For legal compliance: GLBA/HIPAA/State Privacy laws

Security Breaches Summary

- 1572 security breaches involving sensitive personal information were reported in 2012
- Representing over 200 million records
- 2011: 1088 incidents, 127 million records

Source: datalossdb.org

Security Breaches Year-to-Date

16% - Internal fraud

38% - Hack by external party

13% - Stolen device/documents

27% - Accidental release/disclosure/lost

6% - Other

Source: datalossdb.org

WOLF & COMPANY, P.C.

Types of Security Breaches

- Stolen laptops / computers
- Stolen paper reports
- Hacking incidents
- Vendor mismanagement
- Improper destruction of files
- Lost backup tapes
- Dishonest employees selling information

Cost Per Record

Increased to $233 per compromised customer record in 2012, compared to $202 in 2008

Average total per-incident costs in 2012 were $8.9 million, compared $6.65 million in 2008

Costs are moderated by a strong security posture

Source: Ponemon Institute

Direct Attacks and Exploits

- Technical Vulnerabilities
  - Missing patches
  - Outdated systems and applications
  - Custom exploits, 0-day attacks
- Malware: viruses, worms, trojans, backdoors
- Vulnerable or insecure ports and services
- Compromised user credentials
  - Sniffed, guessed, cracked, or brute-forced

Preventing Technical Exploits

Start with basic technical security controls

Avoid these common pitfalls!

- Null or default passwords
- Missing patches with known exploits
- No firewall or poorly configured
- No up-to-date anti-virus software
- Little or no monitoring procedures

These will prevent “opportunistic” attacks

but NOT **Advanced Persistent Threats** (APT)

Social Engineering

- Targets **people** rather than **systems**
- Attackers often attempt to exploit a person's desire to be helpful
- Threats may be disguised as legitimate entities
- Takes many forms

Types of Social Engineering Attacks

- Pharming
- Phishing
- Spear Phishing
- Vishing (VoIP)
- Physical entry
- Removable media ("baiting")

Many attacks use a **COMBINATION** of technical and social engineering tactics

Preventing Social Engineering

- Training, training, training!
  - Testing with simulated social engineering attacks
- Email filtering:
  - Spam
  - Anti-virus / anti-malware
  - Data Loss Prevention (DLP)
- Web filtering
  - Social media sites
  - Personal email and instant messaging
  - Peer to peer
- Physical security

M.G.L. 93H 201 CMR 17 (MA Privacy Law)

- Goes beyond just notification
- Establishes minimum security
  - 17.03: Duty to Protect and Standards for Protecting Personal Information
  - 17.04: Computer System Security Requirements
- Implementation of standards as of March 1, 2010

Background

- Passed by the Office of Consumer Affairs and Business Regulation on September 19, 2008
- Originally scheduled to be effective on January 1, 2009. Deadline extended to March 1, 2010
- One of the first state privacy laws to go beyond requiring notifications
- Established to make companies assume more ownership of sensitive data and incur penalties if they abuse that access

Who is Affected?

- Any person who owns, licenses, stores, or maintains personal information about a resident of Massachusetts

- Applies to **ANY** organization in possession of personal information of Massachusetts residents, whether or not that business maintains a presence in the state

What is Covered?

Personal Information:

- Means a Massachusetts resident's first name or initial, and last name **in combination with one or more of the following**:
  - Social Security number
  - Driver's license or state ID card number
  - Financial account (not just bank account numbers), credit / debit card number (with or without security / access codes, PINs, or passwords needed to access the account)
- Excludes information lawfully obtained from publicly available information or government records
- Includes employee information, thus requiring almost all organizations in MA and surrounding states to comply

The Following is Covered:

Employee Type Information

- Payroll records
- Health benefits
- Direct deposit records
- 401(k)

Compliance and Enforcement

- **Attorney General Enforcement**

  Attorney General may enforce violations of Chapter 93H via actions brought under Chapter 93A

- **Compliance Standards**

  ISP compliance is judged based on:
  - Size, scope and type of business
  - Amount of resources available to such person
  - Amount of personal information stored
  - The need for security

- **Private Right of Action**

  Although neither the Breach Statute or the Information Security Regulation specifically provides for a private right of action, there are several theories under which one could be brought

#1: Identify the Risks

Identify how the regulation pertains to you:

- What types of information are you retaining?
- How much of it are you retaining?
- Where is the information stored?

#2: Develop the Plan

Regulations require a 'Written' Information Security Program (ISP):

- Identify the Information Security Officer
- Document how the regulation applies to you
- Describe the controls in place to protect the information
- Include how disciplinary measures will be imposed for violations of the ISP

#3: Review Your Vendors

You are responsible for the information you provide:

- Identify which vendors are provided with data covered by the regulation
- Ensure the contract includes clauses stating that the vendor is required to protect the data (contracts must contain language by 3/1/2012)
- Ask the vendor how they are addressing the regulation

What To Require of Your Vendors

- Contractually require compliance with applicable state and federal laws
  - Including Massachusetts Privacy Law
- Maintain a Written Information Security Program
- Limit data access and usage to what's in contract
- Prohibit disclosure to third parties
- Require immediate notification if there is a breach
- Reserve the right to audit

#4: Lock It Down

Once you have determined where the data is:

- Is it stored in a **locked** file cabinet?
- Is there a clean desk policy?
- How about visitors?
- How are the documents destroyed?

#5: User Access

- Everyone should have their own user names and passwords
- Passwords should be somewhat complex
- Ensure that lockout settings are enabled to lock user accounts after bad passwords are entered
- Don’t allow employees to share passwords
- Deactivate user accounts that are no longer needed (i.e. terminated employees)
- Users should only have access to what they need for their job
- Change default passwords provided by vendors

#6: Do You Need Encryption?

- Encryption only required when confidential data is:
  - Stored on portable devices
  - Traveling over the internet
  - Transmitted over a wireless device
  - Stored within backup tapes or online backup services

- Many different open source (free) tools available
  - May cost more in administration and recovery
  - Don’t always protect what is needed
  - Must be very careful on setup

WOLF & COMPANY, P.C.

#7: Update the Network

- Ensure most recent **security patches** are being applied
- Upgrade firewalls and servers
- Consider creating a DMZ within the network
- Consider purchasing intrusion prevention systems
- Consider purchasing strong anti-virus and malware tools on all servers, desktops and laptops. **Ensure virus definitions are updated regularly.**

#8: Train, Train, Train

- Most security breaches are the result of uneducated users
- Employees don’t always understand how they can put the organization at risk
- Train employees to understand not only the costs of data breaches, but also the damage to reputation
- Develop a culture where employees are always looking for potential issues and notifying their department heads

#9: Review the Logs

- Ensure network logs are being generated to monitor activity
- Best to record as much as possible, to help in the event of an incident
- Tools are available to ‘weed’ through all the data, to identify potential attempts to access data

#10: Prepare for a Breach

- Don’t wait until a breach occurs to determine how you will respond
- Similar to a disaster, reputational mistakes can be made very easily without a plan

Incident Response Planning

- Assign responsibility
- Identify what data you possess that would classify as a breach
- List consultants and providers that can help
  - Network consultants / forensic analysts
  - Attorneys
  - Credit monitoring services
- Which government agencies will you need to notify?
- Create a public notification template
- Test the plan

#11: Maintain the Plan

- Program needs to be assessed periodically to ensure that it is working
- Spot checks and audits help to ensure that controls are in place
- Select an annual time period to review and update the program, (perhaps a board or executive meeting?)

In Conclusion

- Security is never 100%, but you should set up as many roadblocks as possible
- Many of the new regulation requirements are just changes to internal controls, and may not require huge cost outlays
- Don’t just “do it” to be secure, controls will also help ensure a stable and effective network
- Don’t be shy about what you did, distinguish yourself from your competition and be proud of the things you implemented

Resources

- **Massachusetts Government**

  Overview of Regulation
  http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

  Frequently Asked Questions
  http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf

  Compliance Checklist
  http://www.mass.gov/Eoca/docs/idtheft/compliance_checklist.pdf

  Formulating a Comprehensive Written Information Security Information Program
  http://www.mass.gov/Eoca/docs/idtheft/sec_plan_smallbiz_guide.pdf

- **National Institute of Standards and Technology**

  Small Business Information Security: The Fundamentals
  http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

Thank You!

QUESTIONS?

Ryan J. Rodrigue, CISA, CISSP
IT Assurance Services Manager
Wolf & Company, P.C.
617-428-5443

rrodrigue@wolfandco.com
www.wolfandco.com