DATA SECURITY/PRIVACY: WHAT YOU NEED TO KNOW (AT A MINIMUM!)

How to Prepare Today and Respond Tomorrow

Presented by:
Janet Byrne Thabit, Esq.
Matuszewich, Kelly & McKeever, LLP
(815) 459-3120
jthabit@mkm-law.com
April 30, 2014

Thousands of organizations have experienced a data breach

- Some have become headline news!
- In 2013, one thing was certain, no target was too small or too large for attackers

A new day, a new data breach…

- "Operation Clandestine Fox"

April 27, 2014 – Microsoft admitted to a huge vulnerability in Internet Explorer that allow hackers to set up malicious websites in order to gain complete access to visitors' PC, provided they visited the page with a IE (version 6 and up). From there, hackers could install apps, break into other accounts and generally use the computer as their own.

- "HEARTBLEED Bug" –

April 9, 2014 – An encryption flaw being called one of the biggest security threats the Internet has ever seen. The bug affected many popular websites and services — like Gmail and Facebook — and could have quietly exposed sensitive account information (such as passwords and credit card numbers) over the past two years.

TARGET

- mid-December 2013 – wide-reaching security breach affecting approximately 110 million consumers
- Stolen data including names, credit/debit card numbers, expiration dates, and PINs
- As of mid-January, over 50 purported class action suits were pending across the nation against Target alleging the retailer was negligent in handling consumer's private information.

The Reality Today

- Data breaches and cyberattacks are increasingly common
- No industry is immune from attack! Media coverage has created a distorted picture of data breaches. The reality is that it's not just retailers that are affected; attacks on point-of-sale (POS) systems have actually been trending downwards over the last few years.
- More companies and government offices are "targets of choice"
- Attacks are from:

  -Hackers looking to profit

  -State-sponsored organizations

  -Upset Employees

  -Hackers looking to wreak havoc

Data Breach Business Risks … That You Can't afford to Ignore !!!

- *"When word of a data breach gets out — as it often does — you may face fines and legal action. Just as importantly, your customers, partners [and constituents] may lose faith in your ability to protect their interests, which can directly impact your reputation and your bottom line. And then there's the further expense of finding out what went wrong, and patching any holes in your defenses." 2014 Verizon DBIR.*
- Reputation
- Bottom Line
- Customer Trust
- The costs of a data breach can be enormous!

Rapid Detection has become as Important as Prevention

- Each day the threat is not detected the level of damage and harm increases
- Locating the source of the harm is becoming more difficult
- Attacks are not limited to personal information:

  -Theft of intellectual property

  -Theft of credit card numbers

  -Theft of business and government information

  -Denial of service attacks

Informative Statistics : Verizon 2013 Data Breach Investigations Report (DBIR)

- -78% of intrusions rated as “low difficulty”
- -69% discovery by external party
- -66% took multiple months to discover
- -75% considered opportunistic attacks
- -80% involved authentication based attacks

Common Attack Patterns

- The Verizon DBIR has, for years, been the best source of insight about the threat landscape. The 2014 report covers over 63,000 security incidents from 95 countries, including 1,367 confirmed data breaches.

- **92% OF THE 100,000 INCIDENTS ANALYZED FROM THE LAST 10 YEARS CAN BE DESCRIBED BY JUST NINE BASIC CAUSATION PATTERNS.**

The Nine Patterns

- Miscellaneous Errors
- Crimeware
- Insider and Privilege Misuse
- Physical Theft and Loss
- Web App Attacks
- Denial of Service Attacks
- Cyber-Espionage
- Point of Sale Intrusions
- Payment Card Skimmers

Municipal government: FOIA and data privacy

<u>Protecting data privacy of private information not otherwise subject to FOIA</u>

- ***Employment records***
- ***Employee Health/Disability records***
- ***Social Security records***
- ***Disciplinary records***
- ***Billing/Payment records containing credit card information***

Key Legal Threats Today

- **FTC enforcement activity**

-misleading consumers by "promising" industry-standard or robust security

-inadequate security protection

- **Shareholder litigation**

-loss of intellectual property or confidential information

- **Data breach class actions**

The Response Clock Has Accelerated

- Historically companies delayed notice until a full forensic analysis was done

  - This provided time to form response plan and manage PR, communications and legal

- Today, increased pressures to disclose

  - Privacy advocates/activists often are unsympathetic to company's requests for more time to form response and often threaten to go public if the company doesn't disclose the breach immediately

  - Insurance plans may require prompt disclosure

Plaintiff Lawyers Hooks

Kaiser Foundation Health Plan Breach (CA):

Learned of breach in September 2011 (external hard drive with unencrypted personal information), obtained the hard drive and completed testing for 5 months, then disclosed breach in mid-March 2012.

California Attorney General's allegations

1. Company failed to install/implement adequate security measures
2. Company misled customers about level of its security
3. Company's procedures were lacking or not followed
4. C-suite and/or board was not adequately apprised of security procedures
5. Company took too long to provide notice of data breach or to respond to an attack

Key Take Away –

The goal of every company/public office should be to eliminate as many of these hooks as possible!

*Recent FTC claim upheld

- Wyndom Worldwide, Inc. – New Jersey federal district court upheld FTC's assertion that it has the right to sue companies found negligent in data breach incidents.
- Landmark test of the agency's authority to enforce data security on U.S. companies under FTC prohibition of "unfair" and "deceptive trade practices"

*Judge Salas, April 2014 (No. 13-1887)

Wyndham's wrongs…

- Allowed employees to use easy-to-guess passwords
- Left systems connected to the internet without a firewall
- Failed to inventory systems regularly, and in some cases didn't even know where its servers were physically located
- Stored credit card information on its servers in unencrypted plain text, essentially leaving it wide open for theft

Class Actions

- Plaintiffs' lawyers are looking to cash in on the increase in data security breaches at retailers, banks, and other institutions
- Most cases brought under combination of claims based on:

  -violation of state data breach notification laws

  -violation of state consumer fraud statutes

  -negligence, negligent misrepresentation

  -breach of express/implied contract/warranties

  -Invasion of privacy

Defense Arguments to Class Actions

- There are ways to fight back against this new breed of alleged class action
- Typical arguments on a motion to dismiss:
  - -Plaintiffs lack standing
  - -Plaintiffs lack cognizable injury
  - -Plaintiffs have no private right of action
  - -Remedial efforts by company moots claim

Defending Against Class Certification

- Lack of Standing

-For Article III standing plaintiffs must suffer injury in fact, not merely conjectural

-most plaintiffs allege damages for risk of future harm

-courts disagree, but trend is against, on whether increased risk of personal data being misused in sufficiently "concrete" for Article III standing

Recent cases

- *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007) ("the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm")

- *Allison v. Aetna, Inc.*, 2010 U.S. Dist. LEXIS 22373, at *19-20 (E.D. Pa. Mar. 9, 2010) ("Plaintiff's alleged injury of an increased risk of identify theft is far too speculative.")

The SCOTUS weighs in…

- Clapper v. Amnesty Int'l USA, 113 S. Ct. 1138, 1147 (2013).
  - Human rights groups and public interest lawyers claimed that the National Security Agency's warrantless wiretapping program violated their First and Fourth Amendment rights.

"**[W]e have repeatedly reiterated that threatened injury must be certainly impending to constitute injury in fact, and that [a]llegations of possible future injury are not sufficient".**

But the dust hasn't settled

- Even after *Clapper*, lower courts still divided
- ***In re Sony Gaming Networks & Customer Data Security Breach Litig***., No. MDL 11-2258, 2014 US Dist. LEXIS 7353 (SD Cal. Jan. 21, 2014) ("Although Sony argues that Plaintiffs' allegations are insufficient because none of the name plaintiffs have alleged that their Personal Information was actually accessed by a third party, *Clapper* does not require such allegations")
- ***In re Barnes & Noble Pin Pad***, 2013 US Dist. LEXIS 125730, at *8 (N.D. Ill. Sept. 3, 2013) (alleged increased risk of identify theft found insufficient for standing under *Clapper*)

Key Defensive Steps

- **Privacy Audit and implementation** – ?? where is data coming in/out, how used, what controls, does practice align with policy, training, disclosure plan/practice
- **Risk Assessment** – ?? Identify types of personal information that could be compromised, potential for lost business, fines & penalties, regulatory scrutiny
- **Establish a rapid response team - ??** Identify Key Stakeholders (IT, Legal, security, PR/Communications, HR, risk management, corporate & government relations) and create "playbook" of how incidents will be prevented, handled & disclosed
- **Testing - ??** Assess efficacy & needed improvements, review 3d party vendor contracts, update for changes in the law
- **Evaluation insurance coverage - ??** Assess need for company network security liability, cyber/privacy liability, data loss, business interruption, notice costs

Privacy Audits

- Often performed by a law firm and/or external consultant, knowledgeable of best practices
- External advisors see issues that are hidden to companies
- View each issue from a *"what if"* lawsuit perspective
- *"Good fact"* in the event of litigation
- Provides regulators with comfort

Bottom Line… if You Have, Handle or Store Data…

- **Engage Security Breach Counsel**: Have response team, including counsel such as MK&M who can provide critical legal guidance with respect to your breach notification obligations, in place *before a breach occurs!*
- **Form a Response Plan**: Since a major data security breach puts *any size entity* at substantial risk, prevention is the best defense. Form a breach plan and hire us. While it's probably impossible to prevent every data breach, being able to demonstrate that reasonable care was taken to avoid the risk will help reduce company liability.
- **Monitor and Test**: Consistently monitor system access, perform patches, enforce password policy and test procedures to ensure data protection.