

Cybersecurity in Nonprofits

Michael B. Hayes

Priya Roy

David F. Herman

Cybersecurity is a **HOT** issue...

Banking industry security protocol falters in third-party vendor contracts

ATT Customer Info Exposed by Third Party Data Breach

Neglected Server Provided Entry for JPMorgan Hackers

Scottrade Hit With 1st Data Breach Suit

Wall St. Is Told to Tighten Digital Security of Partners

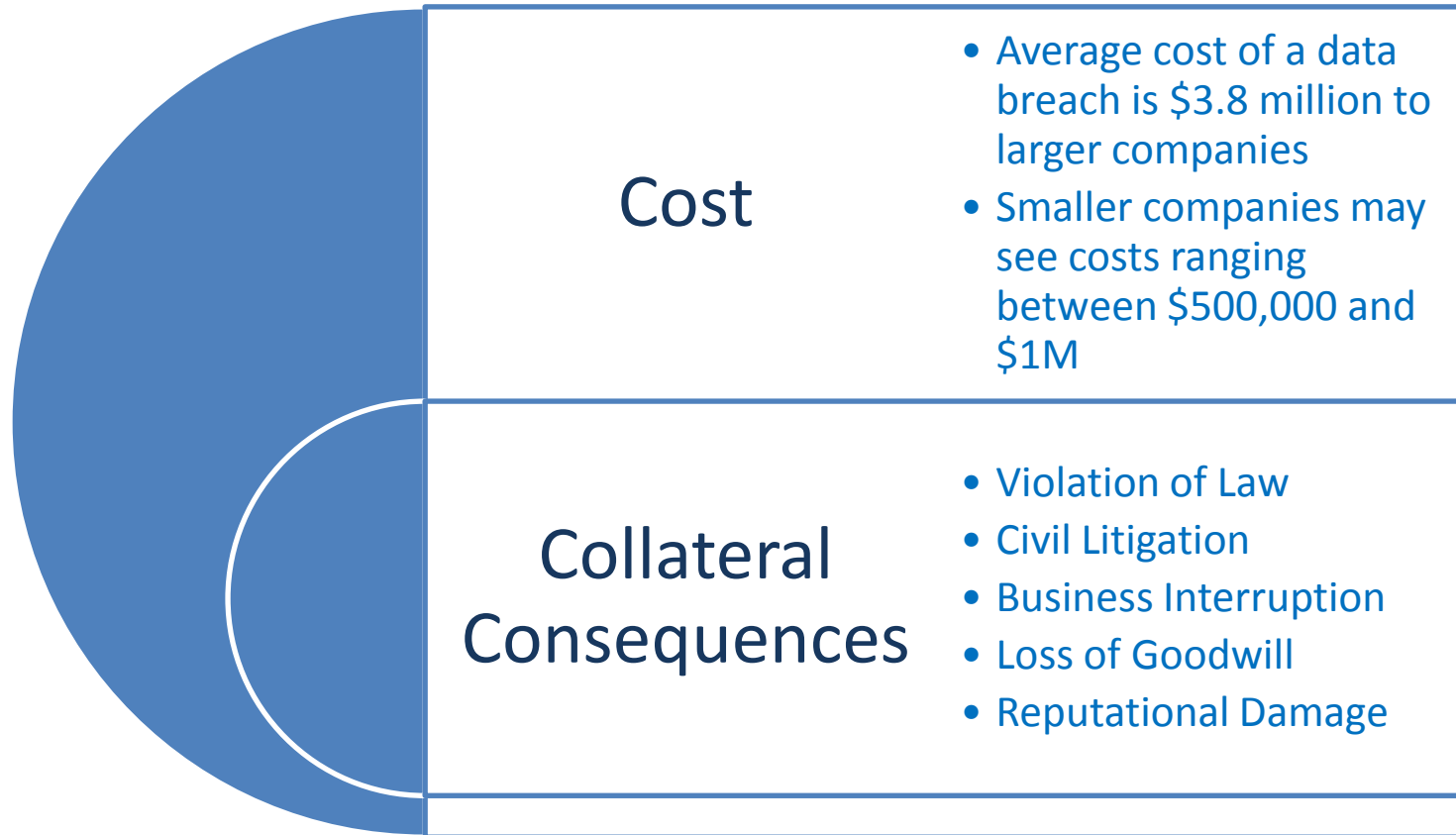
Lowe's Acknowledges Third Party Data Breach

Regulators in the financial services industry are leading the charge in focusing on due diligence of third-party suppliers.

Key Facts About Data Breaches

- Globally, **one billion data records** were **compromised in 2014 – 2015**
- Government **regulators**, most recently the SEC, are beginning to **step up enforcement activity**
- **Businesses are focusing on** all aspects of their data security, including third-party vendors, contractors, and **suppliers**

Impact of Data Breach



Defining Data Breach

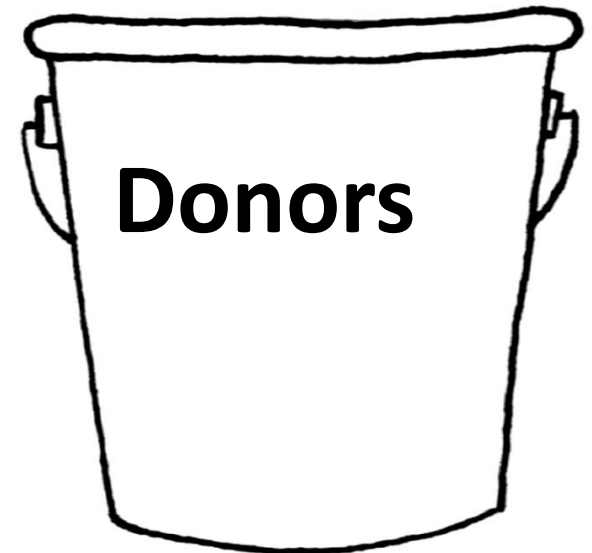
- An Incident in which Secure, Sensitive, Protected, or Confidential Data has been released to or accessed by individuals not authorized to view the data
- Includes not just digital media, but also physical data and devices



Sources of Data Breaches

- External Threats: hackers, cyber-espionage, webapp attacks, malware
- Internal Threats: employee mistakes, physical loss/theft, purposeful misuse, social engineering
- Public Perception vs. Hard Facts
 - Majority of headlines focus on external breaches
 - Employee errors and purposeful misuse account for overwhelming majority of actual breaches

Nonprofits: Three Sources of Data



Personally Identifiable Information

- Broad definition of what constitutes PII
 - Generally an individual's name PLUS at least one other piece of identifying information such as SSN, account number, driver's license number, etc.
- Definition of PII can expand based on state/federal laws:
 - E.g., dates of birth, mother's maiden name, medical information, insurance information, username or e-mail address and passwords

One Example of State Law Definition of PII: Pennsylvania

- Pennsylvania defines PII as:
 - (1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:
 - (i) Social Security number.
 - (ii) Driver's license number or a State identification card number issued in lieu of a driver's license.
 - (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.
 - (2) The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records. (73 P.S. §§ 2301, *et seq.*)
- Applies to records of all PA citizens, *regardless of state where records are stored.*

Developing a Cybersecurity Program

- Data Assessment
- Risk Assessment
- Policy Development
- Implementation

Comprehensive Assessment of Your Organization's Cybersecurity Landscape

- Purpose is to classify data
- Who is the Data being collected from
- How is Data Collected
- Types and Use of Data

Comprehensive Assessment of Your Organization's Cybersecurity Landscape

- Where is PI stored
- Who Has Access to PI

Comprehensive Assessment of Your Organization's Cybersecurity Landscape

- Different types of data are subject to differing levels of protection
- Look to the statutory and regulatory framework to determine how your policies should treat different kinds of information

Key Laws and Regulations

- No single state or federal standard
- Federal Laws
 - FTC Act
 - Gramm-Leach-Bliley Act – 15 U.S.C. § 6801 *et seq.*
 - FCRA - Red Flag Rules
 - HIPAA, FERPA, COPPA, and more...
- State Laws – A patchwork
 - Wide variations in applicability of laws outside of state borders
 - Wide variations in definitions of PII
 - Wide variations in definitions of breach
 - Wide variations in duties imposed by law

Federal Laws

- Laws regulate specific industries and associated companies
- Congress delegates enforcement to numerous agencies:
 - FTC, CFPB, SEC
 - Agency policies and regulations vary dramatically
- Proposed legislation – Cybersecurity Information Sharing Act (“CISA”) of 2015
 - Data Security and Breach Notification Act of 2015
 - Consumer Privacy Protection Act of 2015

Statutory Framework: Affirmative Duties

- Some statutes impose an affirmative duty
 - Imposes an “affirmative and continuing obligation” on companies “to protect the security and confidentiality of those customers’ nonpublic personal information.”
 - Develop, implement, and maintain a written information security program that is appropriate to the individual company
 - Continually conduct risk assessments and update policies as necessary to protect against threats
 - Applicability of certain statutes depends on the types of tasks performed by the non-profits

Red Flags Rule

- Requires an Identity Theft Protection Plan
 - Must identify ‘red flags’ of identity theft likely to be seen by your organization
 - Unique risk assessment of day to day operations
 - Implement procedures necessary to detect ‘red flags’
 - Policies to respond to ‘red flags’
 - Ongoing assessment and refinement of policies
- Can apply to nonprofits across all industries
 - By accepting multiple payments pledges where donors provide bank account or credit card information

Recent Enforcement Actions

- Recent trend by some agencies is to bring enforcement actions where a breach *may* have occurred
- Focus on affirmative compliance rather than *ex post* analysis on the cause(s) of a specific breach
 - Enforcement action brought despite no evidence that data was actually compromised or a customer suffered any financial harm as a result of the cyber-attack
- Focus on third-party breaches

SB 754: Cybersecurity Information Sharing Act (“CISA”) of 2015

- Passed in Senate on October 27, 2015
- Purpose of the Act is to allow companies to share personal information with the government, specifically cyber security threats, even if it violates their own privacy policies
- Primarily concerned with monitoring and reporting of cybersecurity threats
 - Permits active monitoring of threats
 - Permits use of defensive measures to protect against threats
 - Sharing of threat information to and from state and federal government
 - Liability shield provision

State Laws: A Comparison

California (Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.*)

- Notification provisions apply to persons or businesses that conduct business in CA. Data security provisions apply regardless of where data is stored
- PII defined broadly
- Full encryption exemption
- Requires reasonable steps to securely dispose of PII
- Requires (by contract) third-party data security
- Private right of action to CA residents
- Detailed notification made in most expedient time possible
- Large breaches require notice to CA Attorney General

Pennsylvania (73 Pa. C.S. §§ 2301 *et seq.*)

- Law applicable to PA residents regardless of state where data resides
- PII defined narrowly
- Limited encryption exemption
- No private right of action
- Notification by letter, phone, or e-mail (if large enough) “without unreasonable delay”
- Notification where ‘reasonable belief’ of breach
 - Requires active assessment of breach

Example

On November 16, 2015, Anna T. Heft, a volunteer member coordinator for the seventh-best cybersecurity advocacy group in North Dakota (Privacy Experts North Dakota), was distributing information regarding North Dakota's data privacy laws in the local coffee shop. Anna often accessed PEND data on her laptop, especially when she received new member sign-ups and donations. That day Anna spoke with Cy B. Cohen-Lundegaard, a leading advocate for cybersecurity in his hometown of Fargo, North Dakota. Cy expressed his admiration for PEND's goals and wanted to join the organization and make a donation to honor his parents, William Cohen and Frances Lundegaard. As is PEND policy, Anna dutifully recorded all of Cy's information, including that his donation was made to honor his parents, in PEND's donor-list, an excel spreadsheet shared on PEND's unencrypted web server. Anna also entered Cy's credit card information on PEND's encrypted payment portal.

Later that afternoon, Anna returned from the restroom to see that her laptop had been stolen. Anna immediately called PEND to report the theft. None of Cy's account information was compromised, but Cy's name, address, and his parent's names were accessible in the unencrypted donor-list. Has there been a breach of Cy's PII?

State Laws: Unique Provisions

- Some states require notification within a particular time period (i.e. RI within 45 days)
- Some states require offers of identify theft mitigation services to affected residents (i.e. CT)
- Some states require written information security plans (i.e. MA)
- Some states require encryption of storage devices, including laptops and drives containing PII (i.e. NV)


State Laws: The Takeaway

- **BE PROACTIVE:** Patchwork of state laws requires a detailed analysis of the sources and types of information you collect
- **BE VIGILANT:** Nine states enacted changes to their data breach laws in 2015 – more in 2016
- **BE BEST IN CLASS:** Make sure that you have made reasonable efforts to protect your data, clients' data or donors' data – with a goal of being compliant.

Data Assessment and Third Parties

- Next step in Data Assessment is looking at Third Party Vendors
- Third Party control
 - Restrictions on Third Parties
 - Transfer to Third Parties
- What kind data security does Third Party have
 - Liability for actions of Third parties
 - Via contract – ensure compliance of Third parties with your own industry standards

Third Party Cybersecurity is Critical

- FTC, and many others, **require** oversight of third-party vendors and service providers as part of a compliant security program
 - Adequate compliance requires “select[ing] and retain[ing] service providers that are capable of maintaining appropriate safeguards for the customer information at issue.” 16 CFR 314.4(d)(1).
 -  – Documenting in writing all “steps to select and retain service providers capable of maintaining appropriate safeguards and contractually requiring service providers to implement and maintain appropriate safeguards.” CFTC Advisory Letter No 14-21.

Recent Court Cases

- Even if you follow all breach notification laws, you might still face civil liability from individuals harmed in the breach
- Courts are still developing a framework to evaluate these claims, including developing a clear definition of harm necessary to bring a claim
- Courts also struggling with what constitutes reasonable procedures

Target

- Target In re Target Corp. Customer Data Sec. Breach Litig., No. 14-2522, (D. Mn.)
 - Target paid \$10MM settlement to consumers affected by breach.
 - Target paid separate settlements to credit card companies and is still in litigation with financial institutions affected by the breach.
- Type of Hack
 - Hack of Target's computer system through third party
 - Personal and payment card information of about 110 million people affected
 - Consumers alleged injuries such as unlawful charges, late payment charges, and new card fees.

Neiman Marcus

- Hack occurred sometime in 2013
- Neiman did not report until 2014
- Focused whether plaintiffs had been harmed by the data breach
- Definition of “harm” is a moving target

Wyndham

- Based on harm caused by third party affiliates
- Practice what you preach
- Industry standard protocols expected

NIST Cyber Security Framework

- National Institute of Standards and Technology (“NIST”) Cybersecurity Framework
 - <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>
- Core Functions about risk assessment and mitigation
 - Identify, Protect, Detect, Respond, Recover
- Contains “Implementation Tiers:”
 - Companies select appropriate Cybersecurity posture from “Partial” and reactive (Tier 1) to “Adaptive” and risk-informed (Tier 4)
- Profile: The outcomes selected based on business needs—
 - can be used to identify opportunities for improvement and goal setting

Data Assessment: Retention and Disposal Policies

- Disposal of PI
 - Shred
 - Destroy electronically
- Retention Policies
 - Only as long as needed for business purpose
 - Comply with applicable statutes retention policies
 - Keep no longer than required
 - Destroy if required to destroy

Assessment of Risks

- If you don't have a written plan, develop one!
 - Having looked at the types of data you collect – take a look at the statutory scheme to assess risk
 - Where are your holes?
 - What is needed to comply with regulations and laws?
 - What happens if a breach occurs?
 - Determine what levels of protection your data requires
 - Fill holes identified in your risk assessment
 - Develop a plan to monitor and protect against new risks
 - Monitor changes to state/federal laws

Assess Risks: Cybersecurity Best Practices

- Key Takeaways:
 - **Designate** cybersecurity employee or committee to monitor and oversee your policies and procedures
 - **Develop** a written plan and/or contractual agreement with the financial institution detailing how you will prevent, mitigate, and report a data breach
 - **Monitor** cybersecurity threats, vulnerabilities, and legal updates regularly
 - **Ensure** access rights to sensitive data stored in your system is granted only where necessary
 - **Train** employees on the importance of cybersecurity and policies and procedures
 - **Conduct** periodic risk assessments at regular intervals
 - **Isolate and encrypt** sensitive data and PII



Responding to a Breach: Crisis Management

- Not a question of ‘if’ but ‘when’ a breach will occur
- Key Steps for Incident Response:
 - **Diagnose** and **fix** the issue that caused the incident
 - **Prevent** further unauthorized access, intrusion, or disruption of systems and information.
 - **Identify**, if possible, the specific source and cause of the incident
 - **Preserve** potentially relevant evidence for follow-on investigation and analysis
 - Secure compromised systems and devices
 - Determine the individuals and types of information affected
 - Identify all security systems and countermeasures in place at the time of the incident

Responding to a Breach: Incident Response

- Determine your legal obligations
 - Determining your data breach notification requirements is only one aspect of this step. Other aspects include:
 - Federal and state agency reporting requirements
 - Law enforcement notification and cooperation
 - Insurance requirements
- Prepare your internal and external communications regarding the incident
 - Your PR response to the incident should be closely coordinated with counsel.
 - Consider the potential impact of statements on your ability to effectively investigate the incident and prevent the occurrence of similar incidents in the future.

Responding to a Breach: Post-Breach Compliance and Assessments

- **Conduct post-breach analysis:**
 - How and why did breach occur despite previous security assessments? What needs to change?
 - How well did pre-breach policies, procedures, and training function in a crisis situation?
 - Were pre-breach policies and procedures followed?
 - How can policies, procedures, and trainings be improved in the future?

Create Policies and Procedures

- Establish written incident response plan
- Train all employees to identify and report risks and actual breaches
- Designate and train employees to respond to a breach
- Know where to get help

Key Takeaways

- Focus is now on full, proactive compliance, rather than just preventing breaches
- A comprehensive cybersecurity plan is essential to any business plan





Thank You!

Question Session

**Montgomery McCracken
Data Privacy and Cybersecurity**

Michael Hayes | mhayes@mmwr.com

David Herman | dherman@mmwr.com

Priya Roy | proy@mmwr.com

www.mmwr.com | privacyblog.mmwr.com