Understanding Risk Assessments

Key issues in managing data privacy risk and implementing measures to combat security threats

Jim Giszczak and Dom Paluzzi
McDonald Hopkins PLC

beazley

McDonald Hopkins PLC
Attorneys at Law

Objectives

- This webinar will discuss components of the risk assessment and areas to focus on, including these:
  - Identifying the quantity and location of PII/PHI/PCI and which users have access to it
  - Categorizing threats and vulnerabilities
  - Executing a process for secure storage, destruction and disposal of sensitive information
  - Developing a comprehensive written information security program (WISP)
  - Implementing a robust incident response plan and team
  - Vetting third-party services providers with access to PII/PHI/PCI and ensuring vendor compliance
  - Conducting ongoing cybersecurity awareness and training

What data must be protected?

- Personally Identifiable Information (PII)
  - Social Security number
  - Drivers license number
  - Credit/debit card numbers
  - Passport number
  - Bank account information
  - Date of birth
  - Medical information
  - Biometric data (e.g., fingerprints)
  - Mother's maiden name
  - E-mail/username in combination with password/security question and answer

In combination with name (either First Name & Last Name *or* First Initial & Last Name)

What data must be protected?

- Protected Health Information (PHI)
  - Medical records
  - Health status
  - Provision of health care
  - Payment for health care

HIPAA

What data must be protected?

- Payment Card Information (PCI)
  - Primary account number (PAN)
  - Cardholder name
  - Expiration date
  - Service code (3 or 4 digit code)
  - PIN

The who, what, when, where, why and how of risk assessments

Who should conduct a risk assessment?

- Organizations and entities that own, license, store, maintain, have access to, transmit, acquire or use PII/PHI/PCI
- Every industry
- Every size
- Required within many industries and by proposed bills

What is a risk assessment?

- The process of identifying threats and vulnerabilities and the impact on the organization
- Answering the question: “What can go wrong?”
- Technical and legal components

When should a risk assessment be conducted?

- With some frequency, especially when new threats and vulnerabilities are identified
- Trend is for "annual" risk assessments

Where should a risk assessment be conducted?

- On-site at the organization itself
  - Even if utilizing third party services providers to assist
- Several key stakeholders should be involved in the assessment process
  - IT
  - Legal
  - HR
  - Risk
  - Administration

Why should a risk assessment be conducted?

- A risk assessment better positions an organization to address and respond to threats and vulnerabilities
- It is required for some (and may be required under proposed bills)

How should a risk assessment be conducted?

- The methodology for a risk assessment will vary based on the organization and industry
- One size does NOT fit all
- Technical and legal risk assessments
- NIST 800-30
- ISO 27001/27005
- Data Privacy Risk Assessment Questionnaire (*see handout*)

A deeper dive into risk assessments

Identifying threats and vulnerabilities

- Every organization has unique threats and vulnerabilities
- Leverage commonalities
- Threats
  - Human & non-human
  - Internally & externally
  - Can't control attempted threat; can control response
  - Hackers, theft, technical glitches, rogue employees, negligence
- Vulnerabilities
  - Can control
  - Weak passwords, absence of employee training and awareness, lack of access controls, improper or deficient safeguards and policies, inadequate network security management, unpatched systems

Qualitative and quantitative components

- Qualitative
  - High, medium, low
  - Addressed, not addressed, in progress
- Quantitative
  - Cost to the organization should a specific threat occur (single loss and annual loss)
  - Exposure to organization's assets should a threat occur (percentage)
  - Anticipating a specific threat will occur and impact to a specific asset

Critical questions to answer

- What type of PII/PHI/PCI data does the organization have?
- How much PII/PHI/PCI data does the organization have?
- Who has access to the organization's PII/PHI/PCI data?
- Where is the organization's PII/PHI/PCI data stored?
- How is the organization protecting its PII/PHI/PCI data?

Implementing measures to combat security threats

Destruction/disposal laws and document retention issues

- 32 States have data disposal / destruction laws
- A business that maintains records which contain PII concerning customers and employees of the business shall take reasonable measures to ensure the destruction of those records when the business decides that it ***no longer has a legitimate business reason to maintain***
- **Destruction** = Shredding of the record containing PII or erasing the PII from the records
- The failure to destroy unnecessarily increases the number of records in a breach
- AG can impose fines/penalties

Written information security program (WISP)

- Required by Massachusetts law, GLBA and FTC Red Flags Rule
  - Proposed NY regulation
- A program that creates effective administrative, technical and physical safeguards for the protection of PII and PHI
  - Sets forth the organization's procedure for evaluating its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII and PHI.

Incident response plan (IRP)

- The “go to” document
- Identifies the Incident Response Team
  - Roles & Responsibilities
  - Internal & External Capabilities
  - Contact Info (work, cell, home)
  - Alternates
- Decision Trees
- Notification/Escalation Process
- Incident Reports for Gathering Evidence
- Test IRP & IRT

Incident response team (IRT)

- Because the issue impacts almost every component of the organization, and failure to properly manage can result in both long and short term consequences, the team should include "C" level decision makers in the following areas:
  - Legal
  - IT
  - Risk Management/Insurance
  - HR
  - Marketing
  - Public Relations
  - Compliance & Internal Audit
  - Physical security
  - Other executives, as appropriate
  - 3rd party response services (e.g., forensics, privacy counsel, notification/call center, crisis communications)

Cybersecurity awareness and training

- Directly reduces breach costs
- Must be ongoing
- Get creative with awareness
  - Think "outside the box"
  - Posters
  - Sticky notes
  - Cartoons
- Keep record of training
- Implement interactive quizzes (and record passage)

Other privacy policies

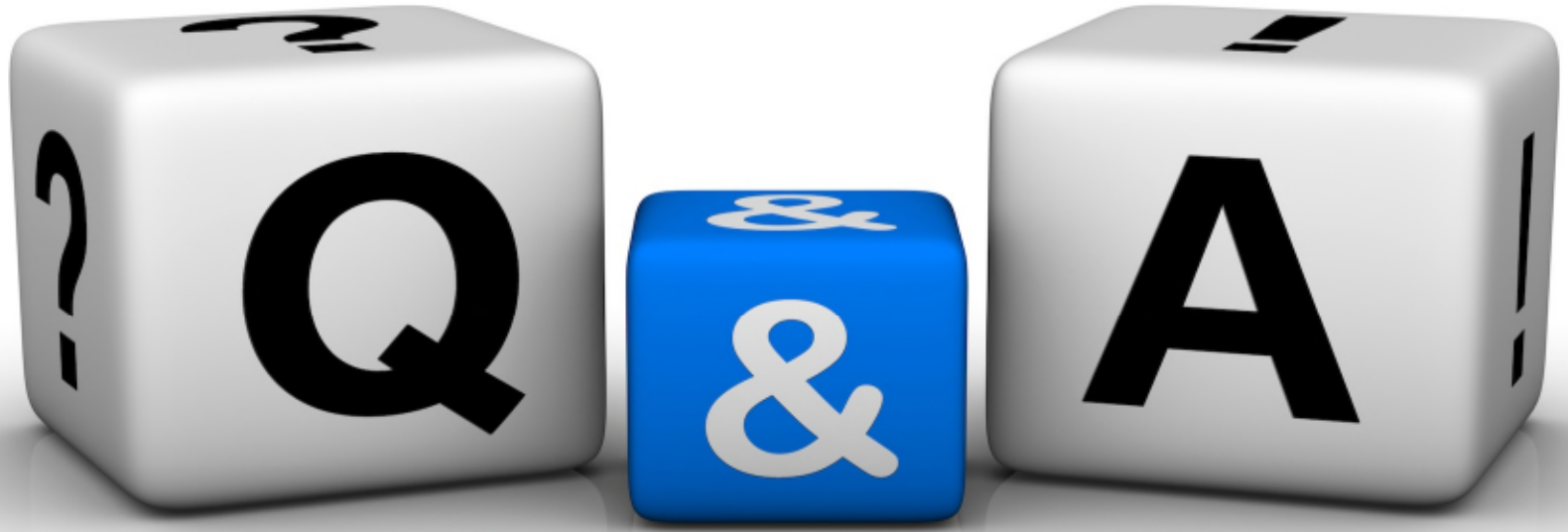
- Computer and electronic devices usage
- Document retention and destruction
- BYOD
- Telecommuting
- Social media
- Website privacy policy and terms of use
- Physical and logical access security

Vendor agreements

- Compliance with data privacy standards for the protection of PII, PHI and/or PCI
- Return or destruction of PII, PHI and/or PCI
- Use of subcontractors with access to PII, PHI and/or PCI
- Notice of security and/or privacy incident within _____ hours
- Indemnification
- Cyber liability insurance

Recommendations for consideration and implementation

- Review records and databases to determine if the organization owns, licenses, stores or maintains PII/PHI/PCI
- Ensure that that the amount of PII/PHI/PCI collected (and time) is limited to the amount (and time) reasonably necessary to accomplish legitimate business purposes
- Limit access to PII/PHI/PCI records to those persons who have a "need to know basis"
- Require ongoing employee training
- Invoke disciplinary measures for violators of data privacy policies
- Put in place secure authentication protocols
- Encrypt all PII/PHI/PCI records and files in transit and at rest
- Implement a comprehensive WISP and IRP
- Update vendor contracts for data privacy compliance



Thank you for your time!

James J. Giszczak
248.220.1354
jgiszczak@mcdonaldhopkins.com

Dominic A. Paluzzi
248.220.1356
dpaluzzi@mcdonaldhopkins.com

Disclaimer

The descriptions contained in this communication are for preliminary informational purposes only and should not be taken as legal advice. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., and is available on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd's. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: 0G55497). CBEM517_US_11/16