CBIZ & MHM
Executive Education Series™

Case Studies in Cybersecurity: A Primer for Not-for-Profits

Ray Gandy & Michelle White

May 2, 2018

About Us

- CBIZ & MHM is a Top Ten accounting provider
- Offices in most major markets
- Tax, attest and advisory services
- Over 2,900 professionals nationwide
- International professional network with Kreston International

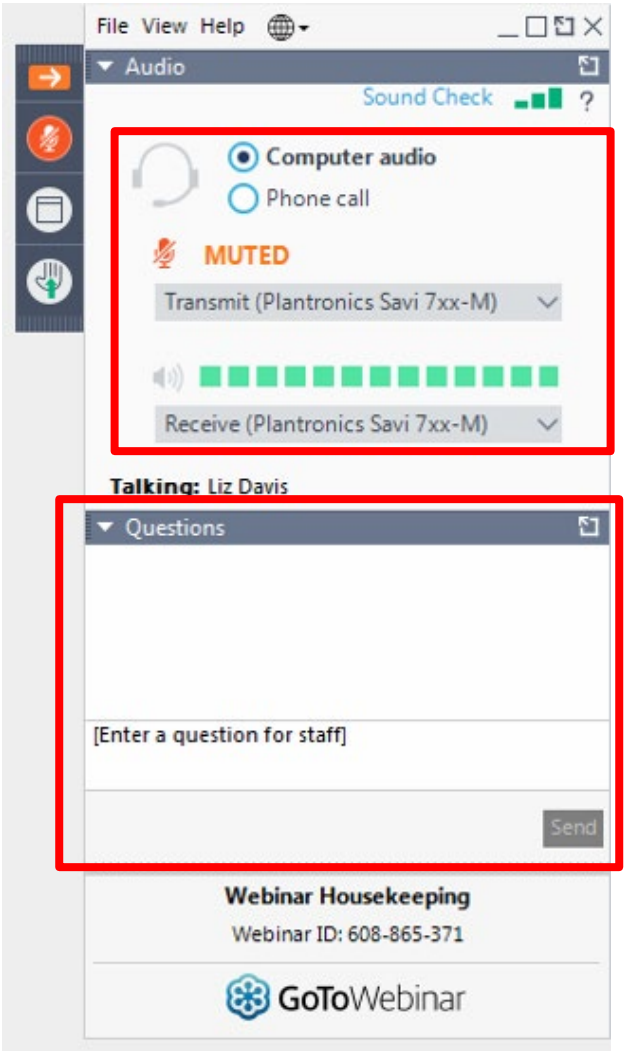
A member of Kreston International
A global network of independent
accounting firms

MHM (Mayer Hoffman McCann P.C.) is an independent CPA firm that provides audit, review and attest services, and works closely with CBIZ, a business consulting, tax and financial services provider. CBIZ and MHM are members of Kreston International Limited, a global network of independent accounting firms.

Before We Get Started…

- Original Broadcast - Use the control panel on the right side of your screen to:
  - Change your audio mode
  - Submit questions
  - Download handouts
- Rebroadcast:
  - Listen through your computer
  - Email questions to cbizmhmwebinars@cbiz.com
  - Click blue handouts icon
- If you need technical assistance:
  - Call support at 877-582-7011
  - Email us at cbizmhmwebinars@cbiz.com

Original Broadcast:



CPE Credit

This webinar is eligible for CPE credit. To receive credit, you will need to answer polling questions throughout the webinar.

External participants will receive their CPE certificates via email within 15 business days of the webinar.

Disclaimer

The information in this Executive Education Series course is a brief summary and may not include all the details relevant to your situation.

Please contact your service provider to further discuss the impact on your business.

Presenters

RAY GANDY, GCCC
Director

Ray has more than 30 years of experience in information technology, including security and controls, strategy, infrastructure, applications, and finance

He is the Leader of the New England IT Risk & Security Practice, and has extensive experience developing and implementing IT security assessments, IT security plans, disaster recovery and business continuity plans, executing large-scale IT integrations, improving operations, optimizing quality, controlling costs, and ensuring customer satisfaction.

617.761.0722 • rgandy@cbiz.com

Presenters

MICHELLE WHITE, CISA, CIPP/E

Manager

Michelle has nearly seven years of experience providing IT risk and consulting services.

She is a member of the IT Risk & Security Practice and has extensive experience improving internal controls, data privacy consulting, developing and implementing strategic plans, identifying operational and financial improvements, and strengthening security. Michelle also has experience with SOC1 and SOC2 audits, SOX 404 readiness and audits, PCI audits, and IPO readiness.

617.761.0664 • michelle.white@cbiz.com

Agenda

01 What's at Risk?

02 Cybersecurity Issues & Examples

03 Solutions & Best Practices

04 Roadmap to Mitigation


WHAT'S AT RISK?

Critical & Sensitive Data*

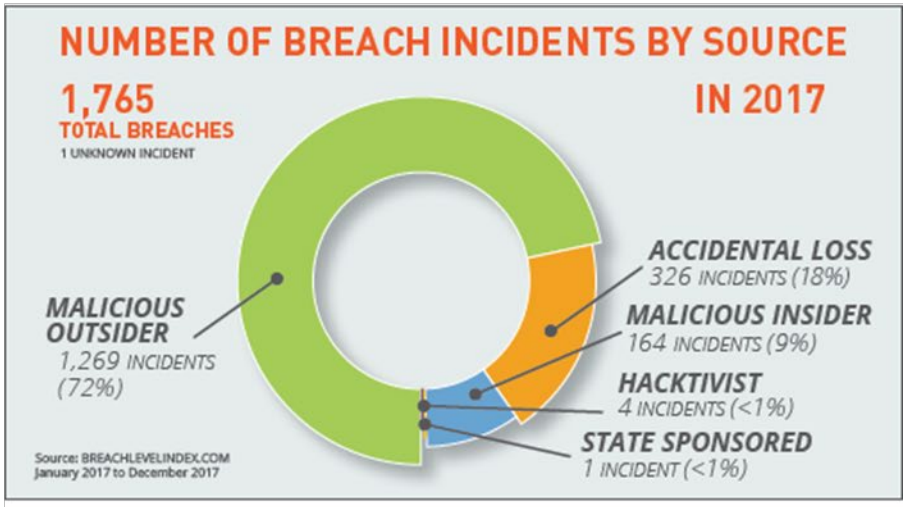
- *Personally Identifiable Information (PII), Social Security Numbers*
- *Finance and Accounting Data*
- *Credit Card or Payment Card Data*
- *Health Information (HIPAA)*
- *Intellectual Property, Research Data, Proprietary Information*
- *Security Information*
- *Generally Confidential Information*

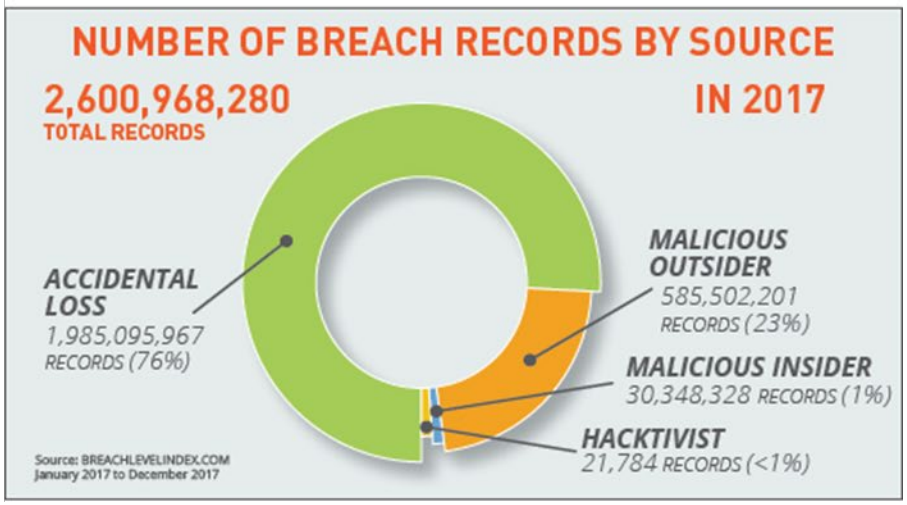
* …Would prove significantly harmful to the business if lost, stolen, damaged or unavailable for a period of time

Risks Resulting from Cybersecurity Exposures

- *Financial Impact*
- *Officer / Director Liability*
- *Regulatory Scrutiny*
- *Brand / Reputation*

2017 Data Breach Statistics





Cybersecurity Issues & Examples

Data Breach Examples

- Password data stolen from other sources (e.g. Equifax, LinkedIn, Dropbox) led to credit card data being accessed and stolen.
- A fake email link (“spear phishing “) clicked on at a development center resulted in employee W2s being stolen.
- An staff member accidentally allowed a hacker access to their system because they downloaded malicious software from the internet.
- Proprietary video content was stolen and released online when the third-party post-production vendor was hacked.

Solutions & Best Practices

Elements of a Successful Enterprise Security Program

- Know Your Threat Vectors and Causes of Failure
- Effective Management & Governance
- Foster the Culture Within the Organization
- Adopt the Policy Framework, Controls & Processes
- Know Your Technology Stack
- Management of Processors, Suppliers, & Vendors
- Effectively Balance Security & Services
- Account for Data Privacy Needs & Requirements

Know Your Threat Vectors and Causes of Failure

- Who (or what) would contribute to the tampering, destruction, or interruption of critical data?
- How do you obtain, store, transmit and process critical data?
- Identify human (e.g., hacktivists) and non-human (e.g., floods) threats
- Quantify/measure risk in terms of motivation, capability & likelihood
- Assess risks through periodic table top exercises & vulnerability testing

Effective Management & Governance

- Security stakeholders should be identified throughout the organization
- Report routinely with leadership, and periodically with the board or Audit/Risk Committee
- Adopt controls to establish consistent language and metrics
- Formalize and centralize policy and procedures
- Build security into the enterprise strategy

Foster the Culture Within the Organization

- Tone at the Top – make it a leadership initiative
- Educate, train and measure continuously the security mindset/culture within the organization
- Include vendors, consultants & partners
- Be proactive (and reactive) using teachable moments and shared experiences
- Ensure policies are reflective of the desired security posture and are fully understood and adhered with

Adopt the Policy Framework, Controls & Processes

- Use a respected security framework. Some examples include:
  - NIST, FFIEC, ISO 27001/2, COBIT 5, ITIL, PCI, CIS 20
- Conduct a baseline/gap assessment with industry professionals
- Be consistent with considering other office locations and devices (e.g. satellite offices or commonly overlooked devices such as printers or security cameras)
- Adopt policies centrally, minimize exceptions to policy
- Prioritize actions consistent with the assessment and improve control attributes that will create positive change

Know Your Technology Stack

- Inventory the devices supporting your business
- Understand what their strengths and weaknesses are, including maintenance or update requirements
- Know where these devices reside physically, and what protections you have in place to protect them
- Have a formalized disaster recovery plan

Management of Processors, Suppliers, & Vendors

- Know what vendors support your critical data
- Adopt a vendor evaluation and management program to ensure the vendor:
  - Keeps your data confidential
  - Follows security 'best practices'
  - Ensures data availability and redundancies
  - Is transparent about 'fourth parties'
- Take advantage of your right to ask questions or audit your vendors and/or obtain and review independent Service Organization Controls (SOC) reports

Effectively Balance Security & Services

- Be transparent with security concerns and options with organization stakeholders
- Adopt “Security by Design” processes and practices into planning stages (rather than reactively)
- Consider mitigating controls or processes prior to making decisions
- Revisit trade-off choices periodically

Account for Data Privacy Needs & Requirements

- Determine whether you are subject to sensitive data or privacy requirements (e.g. state laws, international laws)
- Consider your data collection and retention practices and consider their value to the business in relation to their liability to the business
- Perform Data Protection Impact Assessments when planning for business changes which are of a determined risk nature to individuals (customers or employees)
- Identify Privacy Champions to spearhead privacy thought among business segments

Roadmap to Mitigation

Getting Started

1. Identify critical data – how it originates, where it resides, who has access, how it is secured at rest and in transit

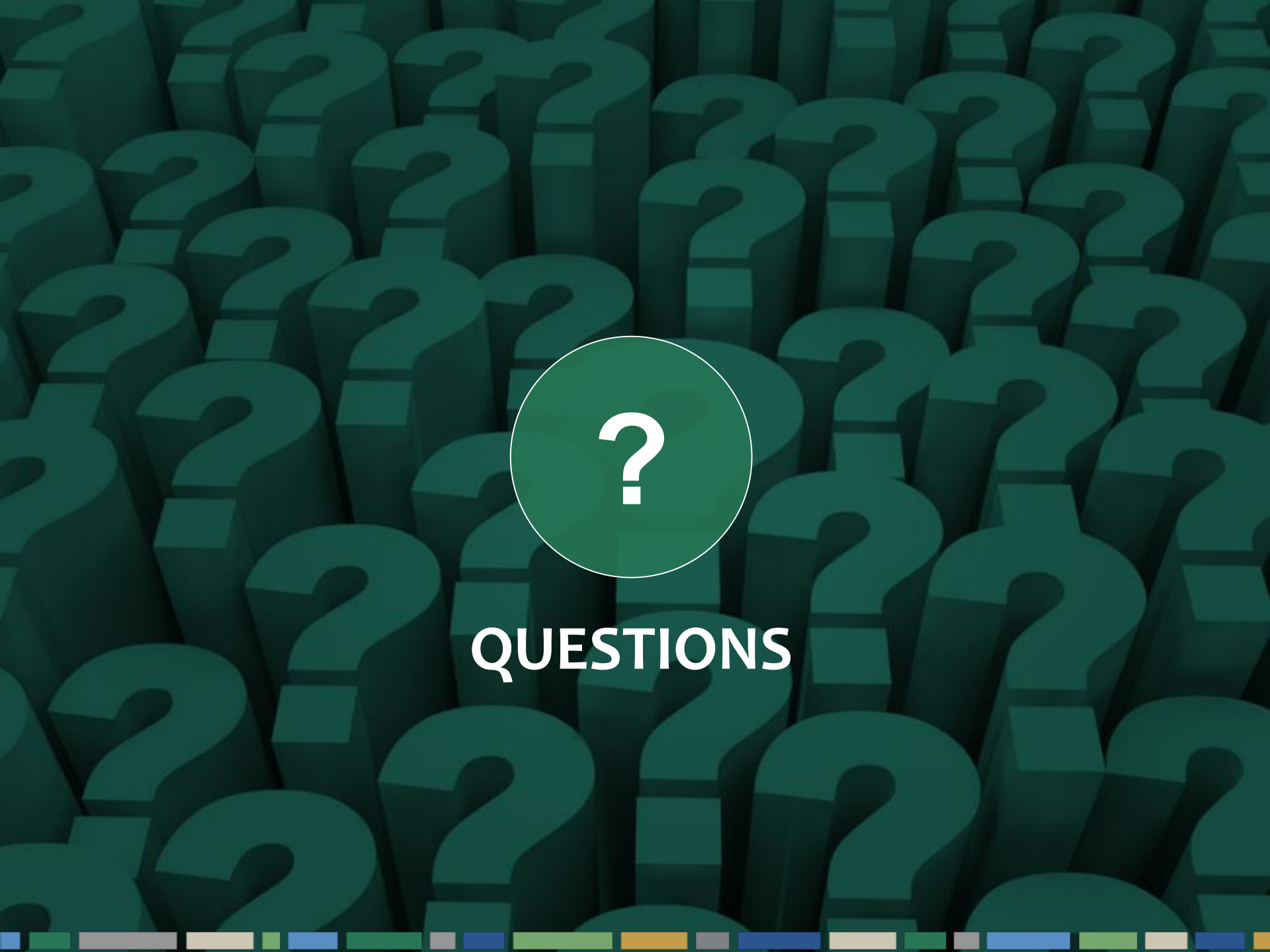
2. Examine the threats and risks to that data

3. Assess yourself against a industry recognized framework and using those results:
   - Establish formality and consistency by adopting controls
   - Identify areas of opportunity for improvement

4. Continually track your progress and evaluate the design and operating effectiveness of your controls

Additional Reading

- How to Tighten Your Company's Cybersecurity
- Privacy Shield Certification 'Adequate' Method for Cross-Border Data Transfer
- Prepare for Tougher European Union Privacy Rules
- Why You Should File Your Taxes ASAP


?
QUESTIONS

If You Enjoyed This Webinar…

Upcoming Courses:

- Check our Executive Education Series homepage for upcoming not-for-profit webinars

Recent Publications:

- Myth Busting the New GDPR and ePrivacy Data Protection Regulations
- Make Your Form 990 A Roadmap for Donors, Board Members, the IRS and the Public
- 8 Ways to Help Prevent a Retirement Plan Lawsuit

Connect with Us

MHM		CBIZ
linkedin.com/company/mayer-hoffman-mccann-p.c.		linkedin.com/company/cbiz-mhm-llc
@mhm_pc		@cbizmhm
youtube.com/mayerhoffmanmccann		youtube.com/BizTipsVideos
slideshare.net/mhmpc		slideshare.net/CBIZInc

THANK YOU

CBIZ & Mayer Hoffman McCann P.C.
cbizmhmwebinars@cbiz.com