Cybersecurity for Nonprofits

MONTGOMERY McCRACKEN
Attorneys At Law

Cybersecurity for Nonprofits

Presenters:

Karen Ibach and David Herman
Montgomery, McCracken, Walker & Rhoads, LLP
123 S. Broad St.,
Philadelphia, PA 19109
215-772-1500
kibach@mmwr.com
dherman@mmwr.com

MONTGOMERY McCRACKEN
Attorneys At Law

Cybersecurity in the News

TECHNOLOGY

Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data

Leer en español

By MIKE ISAAC, KATIE BENNER and SHEERA FRENKEL NOV. 21, 2017

Deloitte

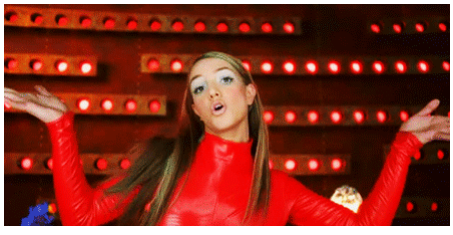
September 25, 2017: A breach that affected Deloitte, a multinational professional services firm, in March came to light—and the reason is pretty embarrassing for a company that was once named the "best cybersecurity consultant in the world" by Gartner. The firm did not employ two-factor authentication, so when hackers acquired a single password from an administrator of the

Executives Step Down as Investigation Continues

By NICOLE PERLROTH and CADE METZ SEPT. 14, 2017

MONTGOMERY McCRACKEN Attorneys At Law

"Oops, [They] Did It Again…."



UBER

MONTGOMERY McCRACKEN Attorneys At Law

Consequences?

MONTGOMERY McCRACKEN
Attorneys At Law

Consequences!

UBER

- AG investigations already open in NY, MA
- More state & federal investigations expected
- Had already settled with FTC for $20M re driver breach

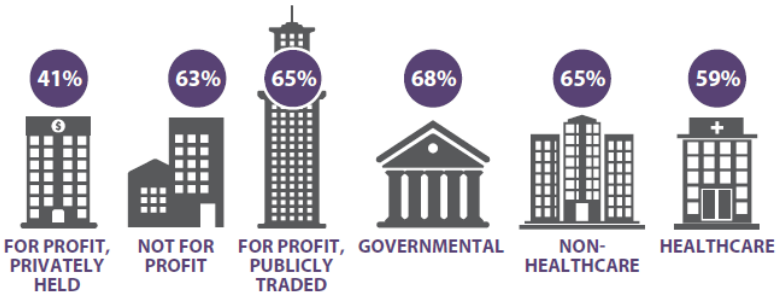
EQUIFAX

- “50 state” complaint combining various lawsuits
- 150 lawsuits nationwide, including suit filed by Chicago
- State & federal investigations expected

MONTGOMERY McCRACKEN
Attorneys At Law

Cybersecurity is a NONPROFIT Issue

Suffered at least one breach in the last year



Society of Corporate Compliance & Ethics / corporatecompliance.org

MONTGOMERY McCRACKEN
Attorneys At Law

Cybersecurity is a NONPROFIT Issue

Nonprofit Nightmare: Data Breach Exposes 10,000 Donors' Financial Records

Wednesday, November 4, 2015 / Categories: **Nonprofit Insurance**

Hacked! Crooks are Grabbing Nonprofit Websites and Demanding Ransom

MARCH 30, 2017 ANDY SEGEDIN

TECHNOLOGY

Small Indiana Nonprofit Falls Victim To Ransom Cyberattack

May 20, 2017 · 8:02 AM ET
Heard on Weekend Edition Saturday

ANNIE ROPEIK FROM IPBS

Malware attacks San Ysidro School District, demands $19K ransom

Posted: Oct 05, 2017 3:25 PM EDT
Updated: Oct 05, 2017 3:43 PM EDT

MONTGOMERY McCRACKEN
Attorneys At Law

Case Study

- Serves cancer patients in a six county area in Indiana.
- Mission is, in part, “to reduce the financial and emotional burdens of those dealing with a cancer diagnosis, as well as promote cancer prevention, early detection and wellness …..”
- Four programs: Nutrients for Life, Miles Toward Health, Medicine for Wellness, and Reaching Out – Breast Cancer; also medical/ comfort supplies, and wigs/ beauty supplies.

MONTGOMERY McCRACKEN Attorneys At Law

What Happened?

- Data goes missing from the server
- Staff get strange text messages about being “new best friends” and “going to help”

Next came the email with the subject line "Cancer Sucks, But We Suck More!"

"It was diabolical. It was cruel," Fant says. "They were brutal."

Hackers accessed the nonprofit's server after a staffer inadvertently downloaded malware from an email. The hackers wanted 50 bitcoin, or what was then about $43,000, to return the data and keep it private.

MONTGOMERY McCRACKEN Attorneys At Law

What Happened?

But Little Red Door doesn't keep anything like that on file, Fant says. So when it decided not to pay the ransom, the hackers posted what they did have.

"It was pretty despicable," Fant says. "We send out grief letters to families [of] clients who have passed away, and they did publish some grief letters – on Twitter."

MONTGOMERY McCRACKEN Attorneys At Law

Aftermath

- Months spent re-entering client information back into the computer system, in some cases from handwritten notes and paper files
- Without data, organization's grant funding seriously impacted – unable to get much of the usual funding

MONTGOMERY McCRACKEN Attorneys At Law

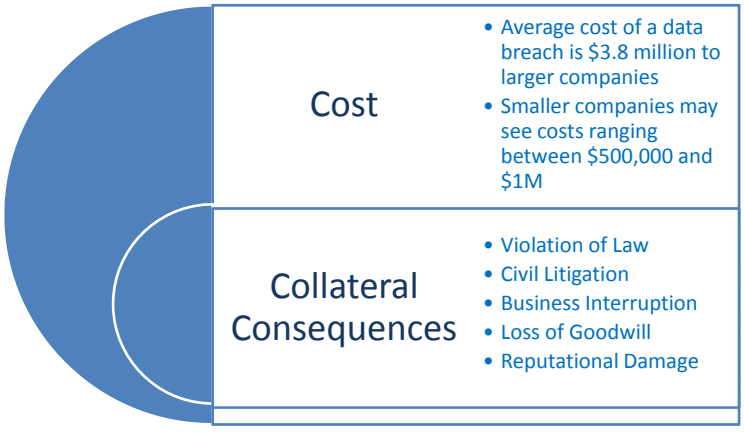
Key Takeaway

No matter an organization's size or scope, data breaches and other cyber crimes can damage:

- ✓ reputation
- ✓ good will
- ✓ assets
- ✓ infrastructure and systems
- ✓ employees
- ✓ clients/customers
- ✓ donors
- ✓ funding
- ✓ vendors, partners

MONTGOMERY McCRACKEN Attorneys At Law

Impact of Data Breach



MONTGOMERY McCRACKEN Attorneys At Law

Don't Wait.
Develop A Cybersecurity Program

- Asses & Address Risks – Know Your Data
- Prepare & Implement Policies and Procedures
- Prepare an Incident Response Plan
- Re-Assess & Re-Address Regularly

MONTGOMERY McCRACKEN
Attorneys At Law

Assessing Risk

MONTGOMERY McCRACKEN
Attorneys At Law

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



MONTGOMERY McCRACKEN
Attorneys At Law

Causes of Data Breaches

- External Threats: hackers, cyber-espionage, webapp attacks, malware, ransomware, spoofing

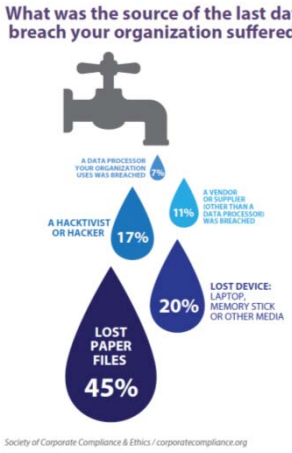


- Internal Threats: employee mistakes, physical loss/theft, purposeful misuse, social engineering, business email compromise



MONTGOMERY McCRACKEN
Attorneys At Law

Public Perception vs. Hard Facts



- Third parties (vendor or data processor) – 18%
- Hackers – 17%
- Lost Device – 20%
- Lost Paper – 45%

Employee errors and purposeful misuse account for overwhelming majority of actual breaches

MONTGOMERY McCRACKEN Attorneys At Law

Assess Your Organization's Cybersecurity Landscape: Classify Data

- Who is the Data being collected from
  - Collected from or about individuals
    - Donors/Sponsors/Grantors
    - Employees
    - Clients
    - Volunteers
- How is Data Collected
  - Website?
    - Online Credit Card Donations?
  - Paper Applications?
    - Employee job applications, intake forms, background checks
- What Types and Use of Data (PII?)

MONTGOMERY McCRACKEN Attorneys At Law

Nonprofits:
Three Sources of Data

MONTGOMERY McCRACKEN
Attorneys At Law

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 password.
  - State laws vary widely.

MONTGOMERY McCRACKEN
Attorneys At Law

Assess Your Organization's Cybersecurity Landscape

- **Where** is PII stored [Electronically? Encrypted? Paper?]
- **Who** Has Access to PII [Employees, Volunteers, Board Members, Third Parties]
- **How i**s access limited or tracked
- 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

MONTGOMERY McCRACKEN Attorneys At Law

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.*
  - 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 definition of breach
  - Wide variations in duties imposed by law

MONTGOMERY McCRACKEN Attorneys At Law

Federal Laws

- Laws regulate specific industries and associated companies
- Congress delegates enforcement to numerous agencies:
  - FTC, CFPB, SEC
  - Agency policies and regulat dramatically

MONTGOMERY McCRACKEN
Attorneys At Law

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

MONTGOMERY McCRACKEN
Attorneys At Law

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

MONTGOMERY McCRACKEN Attorneys At Law

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

MONTGOMERY McCRACKEN Attorneys At Law

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)

MONTGOMERY McCRACKEN Attorneys At Law

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:** Both the States and Federal Government are constantly passing new laws and regulations in this area.
- **GET EXPERT ADVICE IN THE CASE OF A BREACH**: Notification obligations are tricky and complex.

MONTGOMERY McCRACKEN Attorneys At Law

Third Party Cybersecurity is Critical

- Third Party control
  - Restrictions on Third Parties
  - Transfer to Third Parties
- What kind of data security does Third Party have
  - Liability for actions of Third parties
  - Via contract – ensure compliance of Third parties with your own industry standards and maintain appropriate safeguards

MONTGOMERY McCRACKEN Attorneys At Law

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.

MONTGOMERY McCRACKEN Attorneys At Law

Enforcement & Civil Liability

- 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

MONTGOMERY McCRACKEN Attorneys At Law

Policies & Procedures

MONTGOMERY McCRACKEN Attorneys At Law

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

MONTGOMERY McCRACKEN Attorneys At Law

Cybersecurity Best Policy & Procedure Practices

- **Designate** cybersecurity employee or committee to monitor and oversee your policies and procedures
- **Develop** a written plan detailing how you will prevent, mitigate, and report a data breach
- **Monitor** cybersecurity threats, vulnerabilities, and legal updates regularly
- **Update** your software regularly; apply patches
- **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

MONTGOMERY McCRACKEN Attorneys At Law

Policies to Consider, Draft, Implement

- Employee Internet Usage Policy
- Social Media Policy
- Strong Password Policy
- Dual-Factor Authentication
- E-Mail Usage Policy
- Email Retention Policy
- Mobile Device Policy
- Backing up and Storing Data

MONTGOMERY McCRACKEN
Attorneys At Law

Best Cybersecurity Investment?

MONTGOMERY McCRACKEN
Attorneys At Law

TRAIN, TRAIN, TRAIN

- Believe it or not, technological solutions cannot keep up with the changing and evolving threat.
- Internal actors are estimated to be responsible for ***43 percent*** of data loss.
- Training topics can be tailored to needs:
  - Data security and consequences of data loss
  - How to spot a phishing email, social engineering awareness
  - How to Handle Phone Inquires for Information
  - Disposing of Data
  - Avoiding Shoulder Surfing
  - ETC

MONTGOMERY McCRACKEN Attorneys At Law

Culture Matters

SENSE SOMETHING, DO SOMETHING

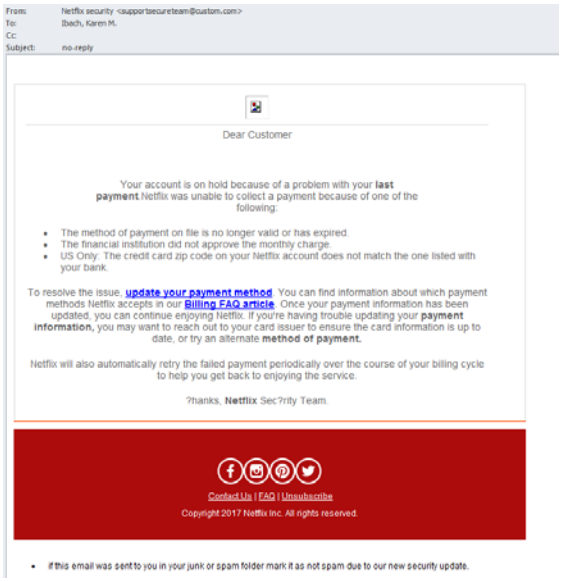
Work to build a culture where everyone understands the risks of cybersecurity, cyber crimes, and data loss, and feels comfortable raising questions or problems.

MONTGOMERY McCRACKEN Attorneys At Law

Very Current Example!

Red Flags:

- ✓ No netflix in return email address
- ✓ Using my work address
- ✓ The ? Marks
- ✓ The request for payment info
- ✓ The links



MONTGOMERY McCRACKEN
Attorneys At Law

Breach: When It Happens ….

You'll Need a Plan ….

MONTGOMERY McCRACKEN
Attorneys At Law

NOT This Plan …

MONTGOMERY McCRACKEN
Attorneys At Law

Breach Response Plan

- 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, and who to call

MONTGOMERY McCRACKEN
Attorneys At Law

Breach Response Plan

- Identify key employees to respond to a breach: PR, IT, Legal, HR, Third Party, etc.
- Require assessment of cause of and scope of the breach along with types of data compromised.
- How can you know how best to respond, if you don't know what you're responding to? Questions to ask:
  - Was data actually exposed during the breach?
  - When was the data exposed?
  - What data was exposed?
  - How many individuals are potentially affected by the breach?
  - Who was the data collected from?
  - Was the data encrypted?

MONTGOMERY McCRACKEN Attorneys At Law

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

MONTGOMERY McCRACKEN Attorneys At Law

Key Steps for Incident Response

- ✓ **Determine** your legal obligations: Type of data exposed will determine potential legal responsibilities of the response.
  - 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

MONTGOMERY McCRACKEN Attorneys At Law

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?

MONTGOMERY McCRACKEN Attorneys At Law

***ESPECIALLY WHEN IT'S SOMEONE ELSE'S CRISIS.**
--Karen Ibach

MONTGOMERY McCRACKEN
Attorneys At Law

Helpful References

FCC's Small Biz Cyber Planner:
https://transition.fcc.gov/cyber/cyberplanner.pdf
(contains numerous additional links to free resources in final appendix, CSL-1-CSL-3)

FTC's Guidance for Small Businesses:
https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
(find additional free resources at https://www.consumer.ftc.gov/blog/2017/10/lets-focus-cybersecurity-small-businesses

MONTGOMERY McCRACKEN
Attorneys At Law

Montgomery, McCracken, Walker & Rhoads, LLP
123 S. Broad St.,
Philadelphia, PA 19109
215-772-7277
dkramer@mmwr.com

MONTGOMERY McCRACKEN
Attorneys At Law