Copyright and Cybersecurity for Nonprofits

Presenters:

Richard Moss and Shawn Li, Ph.D.
Montgomery, McCracken, Walker & Rhoads, LLP

1735 Market Street
Philadelphia, PA 19103
215-772-1500
RMoss@mmwr.com
SLi@mmwr.com

MONTGOMERY McCRACKEN

Copyright Basics

The Congress shall have Power… To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.

U.S. Constitution, Article 1, Section 8, Clause 8

Copyright is a form of intellectual property protection grounded in the United States Constitution.

MONTGOMERY McCRACKEN

Title 17 of the United States Code codifies the Copyright Act of 1976 (effective Jan. 1, 1978), which provides the basic framework for the current federal copyright law.

Under the Copyright Act, copyright protection extends to "**original works of authorship** [published or unpublished] **fixed in any tangible medium of expression**, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."

Copyright Act, Sec. 102

"Original" means the independent creation of the author.

Works of authorship protected by copyright include the following categories:

- literary works (includes computer programs);
- musical works, including any accompanying words;
- dramatic works, including any accompanying music;
- pantomimes and choreographic works;
- pictorial, graphic, and sculptural works;
- motion pictures and other audiovisual works;
- sound recordings; and
- architectural works.

Copyright protection does **not** extend to:

- ideas;
- procedures;
- processes;
- systems;
- methods of operation;
- concepts;
- principles; or
- discoveries.

Although, it may extend to the expression of the foregoing.

However, when there is only one or a few ways of expressing an idea, idea and expression "merge" and even the expression is not protectable (e.g., rules for a sweepstakes contest).

Other forms of IP Protection:

- **Patent:** a limited duration right granted by the government to exclude others from making, using, offering for sale or selling, or importing an invention (i.e., a new, useful and nonobvious process, machine, article of manufacture, or composition of matter as well as improvements to these).
- **Trademark:** a word, phrase, symbol, and/or design that identifies and distinguishes the source of the goods and/or services of one party from those of others.

  Unlike patents and copyrights, trademarks do not expire after a set term of years.

The copyright owner has the exclusive rights to do and to authorize any of the following:

- to **reproduce** the copyrighted work in copies or phonorecords;
- to **prepare derivative works** based upon the copyrighted work;
- to **distribute** copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
- for literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to **perform** the copyrighted work publicly;
- for literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to **display** the copyrighted work publicly; or
- for sound recordings, to **perform** the copyrighted work publicly **by means of a digital audio transmission**.

An original work of authorship is automatically protected under copyright the moment it is fixed in a tangible form.

Registration of a work with the Copyright Office (a separate federal department within the Library of Congress) is **not** a prerequisite for copyright protection.

Federal registration, however, is required before a copyright infringement action can proceed.

Registered works may be eligible for statutory damages and attorney fees and costs in successful litigation. Also, registration is *prima facie* evidence of the validity of the copyright when made within 5 years of publication. And, registration permits a copyright owner to establish a record with U.S. Customs and Border Protection for protection against the importation of infringing copies.

A copyright notice is an identifier placed on copies of the work to inform the public of copyright ownership. The copyright notice generally consists of the © symbol, or the word "copyright" (or abbreviation "copr."), the year of first publication of the copyrighted work, and an identification of the owner of the copyright, e.g., ©2018 Joe Shmo.

Once required as a condition of copyright protection, use of a copyright notice is now **optional**. Also, use of the notice does **not** require permission from, or registration with, the Copyright Office.

For works of authorship created by an individual, copyright protection lasts for the **life of the author + 70 years**.

Authors or their heirs can terminate an agreement that transferred or licensed the author's copyright to a third party after 35 years.

For works of authorship created anonymously, pseudonymously, and for **works made for hire**, protection lasts **95 years from** the date of **publication or 120 years from** the date of **creation, whichever is shorter**.

For works made for hire, termination provisions do not apply.

When deciding to use a work protected by copyright, the general rule is to seek permission from the copyright owner.

However, under the Copyright Act, certain uses of copyrighted works are permissible without first obtaining permission of the copyright owner.

The Copyright Act codifies the **fair use doctrine**, which promotes freedom of expression by permitting the unlicensed use of copyright protected works for purposes such as, for example, criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research.

Whether a particular use is a fair use depends on:

- the purpose and character of the use, including whether it is of a commercial nature or is for nonprofit educational purposes;
- the nature of the copyrighted work;
- the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- the effect of the use upon the potential market for or value of the copyrighted work.

Work Made for Hire

The general rule is that the person who creates the work is its author and the copyright owner. The exception is a **work made for hire**.

When a work qualifies as a work made for hire, the author is not the person who actually created the work. Rather, **the creator's employer or the commissioning party is considered the author and the copyright owner**.

Whether a work is made for hire is determined by the circumstances existing at the time the work is created. A work may be made for hire:

- when it is **created by an employee** (under general principles of agency law, which look to the status and conduct of the employer and the control exercised by the employer over the employee and the work) **within the scope of employment**, **or**
- when a creator (**independent contractor**) and the hiring party enter into an **express written agreement** that it is to be considered a "work made for hire" **and** the work is **specially ordered or commissioned for use** as:
  - a compilation;
  - a contribution to a collective work;
  - part of a motion picture or other audiovisual work;
  - a translation;
  - a supplementary work (e.g., a forward; editorial notes);
  - an instructional text;
  - a test;
  - answer material for a test; or
  - an atlas.

Mere ownership or possession of the created thing itself does not convey any copyright ownership in the underlying creative work.

It is the copyright owner who may direct how and to what extent copies of the work may be made and used.

To determine who owns a work of authorship, the principal inquiry is whether the creator of the work is an **employee** or an **independent contractor**.

If the creator is an employee, the presumption is the employer owns the copyright.

If the creator is an independent contractor, the presumption is the independent contractor owns the copyright -- unless there is a work made for hire agreement and the work falls into one of the foregoing nine categories of specially-ordered or commissioned works.

The work made for hire exception does not apply to volunteers!

When a volunteer creates a copyrightable work, the Copyright Act confers exclusive ownership to the volunteer.

Also, in the area of the visual arts, the Visual Artists Rights Act of 1990 confers to the volunteer creator (regardless of physical ownership of the work itself, and regardless of who holds the copyright) the additional moral rights of attribution, integrity (i.e., the right to prevent distortion, mutilation, or modification that would prejudice the author's honor or reputation), and, for authors of works of "recognized stature," to prevent destruction.

A nonprofit hiring an employee author (e.g., a writer, artist, programmer, designer) should take affirmative steps to secure the copyright in the work product if that is its intention.

This can be accomplished by including in the employment agreement:

- an assignment clause drafted as a **present grant;**
- a back-up work made for hire provision (to minimize the risk that the employee may later attempt to claim ownership);
- a waiver of moral rights clause; and
- a further assurances clause.

To secure work made for hire for an eligible work created by an independent contractor, **a written agreement signed by the parties expressly stating that the work is a "work made for hire" is required**.

The work for hire clause should be accompanied by a back-up present assignment in the event copyright ownership through work made for hire is challenged (note: where copyright ownership is transferred via assignment to the commissioning party, the author or heirs may have the right to terminate the assignment after 35 years).

When dealing with a volunteer creator, the nonprofit can pursue a written agreement to acquire ownership of the work or to license rights in and to the work.

The agreement should include a detailed, expansive, and substantive recitation of the benefits derived by the volunteer to demonstrate that the parties have validly exchanged valuable consideration in good faith.

Ideally, the agreement should require the volunteer to waive any moral rights and to represent and warrant that the work is original and (to the volunteer's knowledge) does not violate third party IP rights.

Cybersecurity for Nonprofits

MONTGOMERY McCRACKEN

Cybersecurity is a NONPROFIT Issue

Cyber Criminals are targeting smaller organizations

- Lack of sophisticated network security

Nonprofits have what Cyber Criminals want:

- Payment information
- Personally Identifiable Information (PII)
- Information of donors, patrons, newsletter subscribers, etc.

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

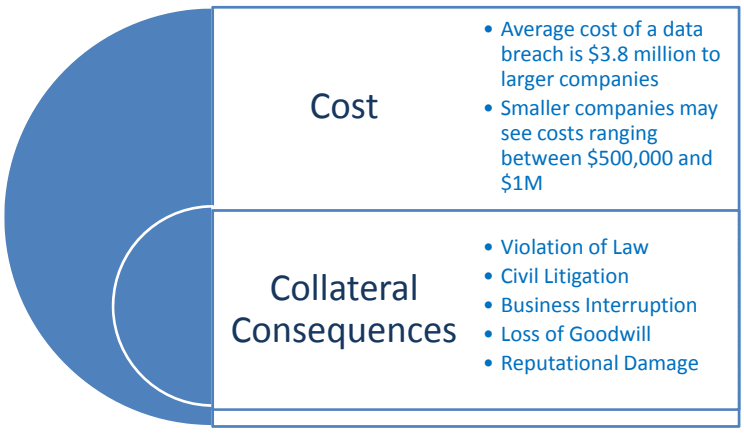
ANNIE ROPEIK

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

Impact of Data Breach



Uncertain Legal Framework

- **NO** single state or federal standard
- Federal Laws
  - FTC Act
  - Gramm-Leach-Bliley Act – 15 U.S.C. § 6801 *et seq.*
  - Red Flag Rules (FCRA)
  - 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

Federal Laws

- Laws regulate specific industries and associated companies (e.g., financial, healthcare, etc.)
- Congress delegates enforcement to numerous agencies:
  - FTC, CFPB, SEC
  - Agency policies and regulation

Red Flags Rule

- **Fair and Accurate Credit Transactions Act of 2003**
- **Apply to Financial Institutions and Creditors**
  - Can apply to nonprofits across all industries
    - By accepting multiple payments pledges where donors provide bank account or credit card information
  - Lawyers, doctors, ... and other service providers [are] no longer classified as 'creditors' for the purpose of the red flags rule
- **Requires an Identity Theft Protection Plan**
  - Must identify 'red flags' of identity theft
  - Implement procedures necessary to detect 'red flags'
  - Policies to respond to 'red flags'
  - Ongoing assessment and refinement of policies

29

Data Security Laws

- More than half the states
- Apply to businesses that own, license, or maintain personal information about a resident of that state
- Requires implement and maintain reasonable security procedures and practices appropriate to the nature of the information
- Protect the personal information from unauthorized access, destruction, use, modification, or disclosure

http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx#DataSecLaws

Data Breach Notification Laws

- All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands
- Who must comply (e.g., businesses, data/ information brokers, government entities, etc.)
- Definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.)
- What constitutes a breach (e.g., unauthorized acquisition of data)
- Requirements for notice (e.g., timing or method of notice, who must be notified)
- Exemptions (e.g., for encrypted information)

http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx#1

Data Disposal Laws

- FTC Disposal Rule
- 34 states and Puerto Rico
- Require either private or governmental entities or both to destroy, dispose, or otherwise make personal information unreadable or undecipherable

http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx

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

- Law applicable to PA residents regardless of state where data resides
- PII defined narrowly
  - first name (or initial) and last name along with
    - social security number,
    - driver's license number (or state ID), or
    - bank information along with the access code or similar codes
- Notification where 'reasonable belief' of breach
  - by letter, phone, or e-mail "without unreasonable delay"
- Requires active assessment of breach
- No private right of action

California Consumer Privacy Act of 2018

- Apply to a for profit business collect "personal information" and profit from consumers in California
- Broad definition of "Personal information"
  - identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
- Consumer Rights
  - Know What Information Is Collected
  - Request Deletion
  - Request disclosures about Personal Information that Is sold
  - Opt Out of the sale of Personal Information

International Laws and Regulations

EU General Data Protection Regulation (GDPR)

- Extraterritorial applicability
  - applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not.
- Penalties
  - Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).
- Consent
  - Consent must be clear and distinguishable from other matters. It must be as easy to withdraw consent as it is to give it.
- Data Subject Rights

International Laws and Regulations

China Data Protection Regulations (CDPR)

- Critical information infrastructure operators (CIIOs) to store personal information and important data collected and generated within the territory of the PRC.
- Regulates cross-border transmitting of personal information and important data
  - Require Consent
  - Require Data Security Assessment

Don't Wait.
Develop A Cybersecurity Program

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

Assess Your Organization's Cybersecurity Landscape: Classify Data

- What Types and Use of Data (PII?)
- 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

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** is 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

Common Attack Vectors

- **Malware:** Programs that introduce malicious codes (viruses, worms, Trojans)
- **Keyloggers:** Employs programs to collect everything that the user types via keyboard. They can even take screenshots.
- **Social engineering:** Obtaining confidential information from a person or organization to use it for malicious purposes.
  - **Phishing:** Deceiving the users to obtain their confidential information by spoofing the identity of a body or Internet website.
  - **Spam:** Email; instant messaging; and unsolicited calls

Common Attack Vectors (Cont'd)

Active Attacks:

- **Spoofing:** Addresses to the use of techniques for identity theft.
- **Modification:** Consists in modifying the routing table so that the sender sends message through longer paths causing major delays.
- **DDoS:** Attack of Distributed Denial of Service (DDoS) is to keep busy consuming network bandwidth with constant messages that disrupt normal service delivery.
- **Fabrication:** False routing message generated to prevent information of reaching its destination.

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

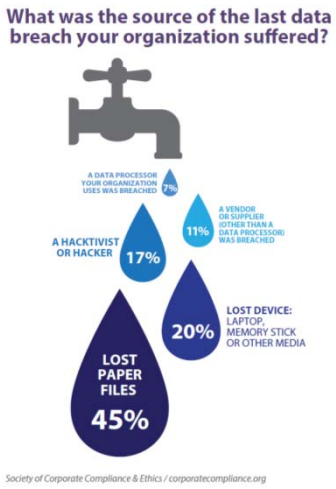


Causes of Data Breaches

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

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

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

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

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 Da

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

Best Cybersecurity Investment?

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

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.

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.

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

Breach: When It Happens ….

You'll Need a Plan ….

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

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?

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

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

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, Walker & Rhoads, LLP
1735 Market St.,
Philadelphia, PA 19103
215-772-1500
RMoss@mmwr.com
SLi@mmwr.com

MONTGOMERY McCRACKEN