Privacy and Incident Response for Higher Education Institutions

Meghan O'Connor
Quarles & Brady, LLP

2021 WACTE Legal Issues Conference
October 28, 2021

Quarles & Brady LLP

Welcome and Agenda

PRIVACY PROGRAM BEST PRACTICES

APPLICABLE PRIVACY LAWS

CYBERSECURITY AND INCIDENT RESPONSE

Privacy Program Best Practices

Privacy and Incident Response for Higher Education Institutions

Quarles & Brady LLP

Best Practices for Privacy Program

- Data mapping
- Remember data security is part of privacy
- Develop vendor diligence/contracting standards
- Develop privacy policies that address array of applicable privacy laws
- Build/update your data retention and destruction program
- Train workforce

What Do You Do With Your Data?

- Do you have a data map?
- Leverage your data map to build out your privacy program
  - Understand what data you have, where you keep it, and what you do with it
  - Employee, student, health, confidential business information/trade secrets
- Why?
  - Data minimization
  - Appropriate safeguards – encryption, role-based access
  - Respond to security incidents
  - Vendor obligations – service provider agreements
  - Respond to individual requests – correct inaccuracies, delete data, obtain a copy, opt-outs, etc.

Data Security is Part of Privacy

- Tabletop exercise – practice and test your incident response policy
- Engage support partners in advance
  - Take advantage of attorney-client privilege
  - Attorney, forensic IT, PR
- Conduct a risk analysis
  - Identify vulnerabilities and risk
  - Inform safeguards

Vendor Diligence

- Develop vendor diligence process
  - Pre-contracting and periodic review
  - What security standards/audits in place?
  - What type of access will they have? Not just type of data
- Determine what vendors touch personal data
  - *e.g.*, SaaS platform, payment processing, website hosting
- Review contracts to make sure they contain adequate privacy and security provisions

Policies and Procedures

- Includes website privacy policy and internal policies
- What are your practices that you follow?
  - Privacy and security
  - Internal access rights
  - Responding to individual requests, verification of identity
  - Handling terminated employees
  - De-identification of data
  - Responding to complaints
  - Timing of assessments, privacy policy review, etc.
- Should match your actual practices
- Comply with all applicable privacy laws and standards
- Future proof for regulator interaction

Data Retention and Destruction

- Trend: No longer keep all data forever
  - Data minimization
  - Data retention must be a reasonable time period
  - Disclose retention period at time of collection (CA)
- Leverage your data map – what do you have and why?
- Destroy data securely
- Do not forget about email and messaging
  - Legal holds
  - Business email compromises are common

Train Employees

- Training on what?
  - General best practice
  - How to handle personal information
  - Different privacy laws
  - Understand responsibilities to protect student and employee data
- Great security investment
  - Do not leave the window open at Fort Knox
  - Human error and phishing
- Culture of compliance

Applicable Privacy Laws

Privacy and Incident Response for Higher Education Institutions

Quarles & Brady LLP

What Laws and Standards Apply?

- State privacy law – personal information
- HIPAA – protected health information
- FERPA – education records
- FTC Act – privacy as a consumer protection issue, prohibits unfair and deceptive trade practices
- Gramm-Leach-Bliley – consumer financial information
- PCI – credit card data

State Privacy Law

- No comprehensive state privacy law in Wisconsin yet
  - California, Colorado, Virginia, and more on the way
  - But industry-specific privacy laws (*e.g.*, health care)
- Data breach notification
  - Obligations depend on residency of individual not location of institution
  - Consider access vs. acquisition
  - Analyze residency of students with in- and out-of-state addresses

Wisconsin Data Breach Notification

- If entity that maintains or licenses *personal information* in Wisconsin knows that personal information in the entity's possession has been *acquired* by a person whom the entity has not authorized to acquire the information, the entity must provide breach notification to *individual*
- “Personal information” includes name in combination with any of the following non-publicly available elements: SSN, driver’s license or state ID #, financial account number (including credit card number) or any related code allowing access, DNA, or unique biometric data
- Notice is not required if acquisition of personal information does not create a material risk of identity theft or fraud to subject individual
- Notice to individuals within reasonable time, not to exceed 45 days after discovery of acquisition
- Notice to consumer reporting agencies if 1,000 or more individuals notified

HIPAA

- Applies to:
    - Most providers
    - Health care clearinghouses
    - Health plans (including self-funded plans)
    - Business associates of covered entities
- Addresses “protected health information” or PHI
    - PHI specifically excludes data subject to FERPA
- Sets a minimum federal standard for use and disclosure of PHI
    - May not use or disclose PHI without authorization unless an exception applies
    - Preemption – state law that is more stringent (e.g., greater individual rights, more protective)

FERPA

- Applies to schools that receive funds from a U.S. Department of Education program
- Addresses education records
  - Very broad definition
  - Excludes treatment records (subset of medical records)
- Gives parents and secondary education students 18 or over with certain rights re: education records
  - Educational institution may not disclose education records or PI from education records without prior consent unless an exception applies

Both HIPAA and FERPA?

- Yes, it is possible
- FERPA
  - All education records
  - Campus health clinic records (education or treatment records)
- HIPAA
  - Health plan records
  - School is a health care provider that transmits PHI electronically in connection with a standard electronic transaction (*e.g.*, hospital on campus)
  - School is a covered entity and provides services to non-students

Cybersecurity and Incident Response

Privacy and Incident Response for Higher Education Institutions

Quarles & Brady LLP

Recent Developments

- FBI/CISA warning on increased ransomware targeting educational institutions (March 16)
- Biden Executive Order on Improving the Nation's Cybersecurity (May 12)
- White House open letter urging private sector to adopt specific best practices to protect against ransomware (June 2)
- HHS OCR and CISA issue cyber alert on ransomware resources and critical vulnerability (June 9)
- NIST releases draft Cybersecurity Framework Profile for Ransomware Risk Management (June 9)

Impact by the Numbers

$4.62 million

Average cost of ransomware breach

20%

Share of breaches initially caused by compromised credentials

$2 million

Average cost savings for organizations with IR teams and IR testing

76% of organizations

Said remote work would increase time to identify and contain a potential breach

80% of breaches

Involve personal information

PI = most frequently compromised data
PI = costliest data at $180/record

287 days

Average number of days to identify and contain breach

$1.07 million

Cost difference where remote work was factor in causing breach

38%

Lost business share of total breach costs

Largest share of breach costs

From Poneman Institute, Cost of a Data Breach 2020 and 2021

Breach Cost Centers

Detection and Escalation

Forensic and investigative activities

Crisis management

Communication to Boards

Notification

Engage legal counsel

Determination of regulatory requirements

Notice to data subjects

Communication with regulators

Lost Business

Business disruption and system downtime

Lost customers and acquiring new customers

Reputational damage

(38% of breach costs)

Post Breach Response

Inbound communications

Credit monitoring

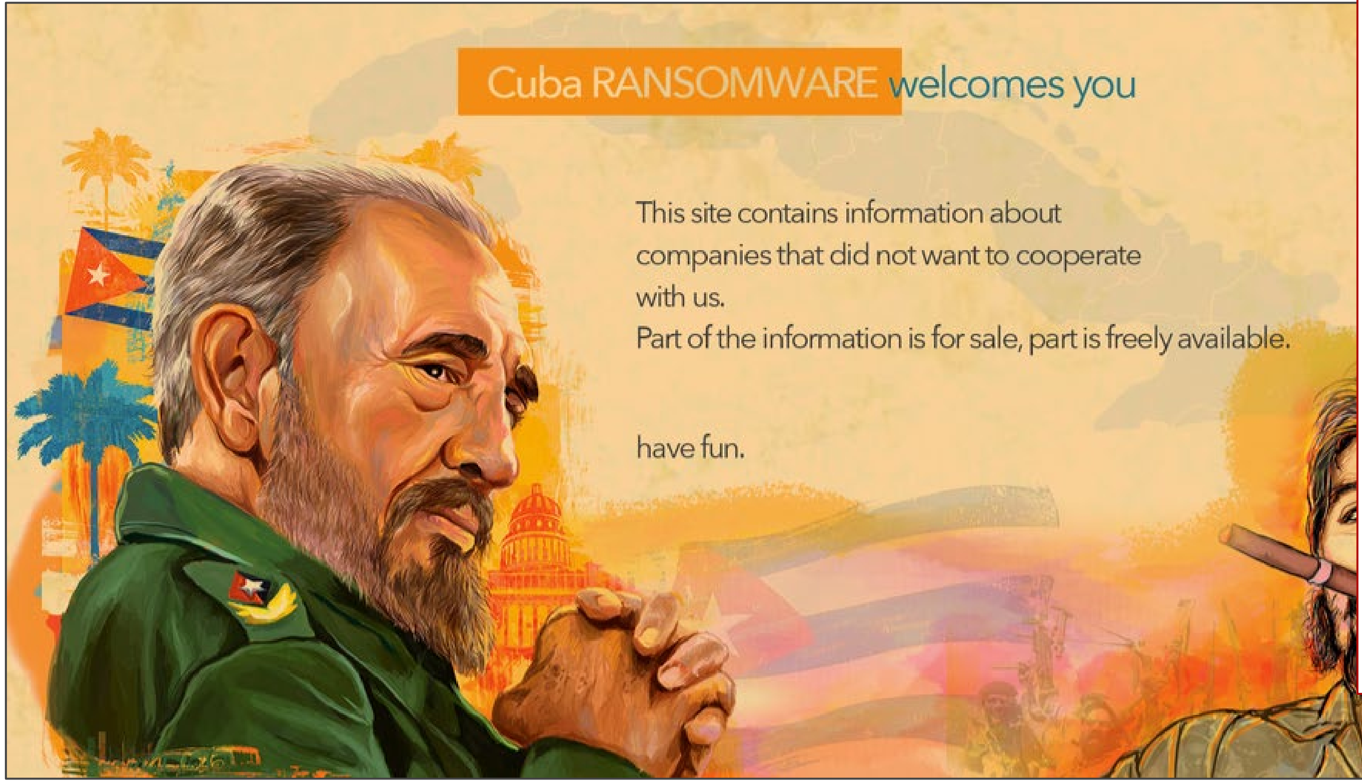
Legal/PR expenditures

Regulatory fine

Mitigation

From Poneman Institute, Cost of a Data Breach 2021

Today’s Changing Risks



Cuba RANSOMWARE welcomes you

This site contains information about companies that did not want to cooperate with us.

Part of the information is for sale, part is freely available.

have fun.

‘Double Extortion’ Ransomware Attacks Spike

Author:
Lindsey O'Donnell

More ransomware operators are setting up pages where they threaten to publish compromised data from victims – an added pressure for victims to pay the ransom.

Today: 77% of all ransomware cases involve data theft

Who's Driving?

Balance competing interests throughout incident response lifecycle

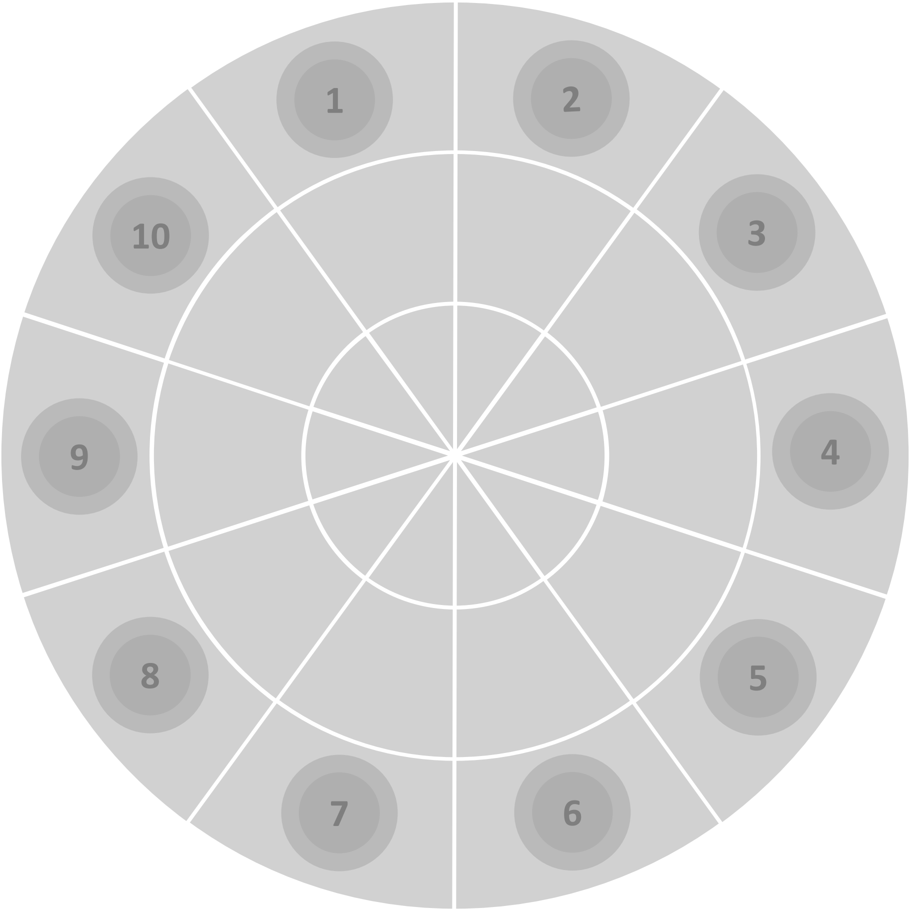
IT/Security
Recovery. Return to operations.
Limit downtime.

Regulators
Identify compliance gaps, confirm appropriate notification to affected individuals, issue penalties.

Internal Compliance Team
Identify compliance gaps.
Follow investigation & notification obligations. Limit regulatory issues.

Internal Stakeholders
Public relations. Financial impact.
Manage appropriate messaging.

Human Resources
Internal messaging. Discipline.
Manage appropriate messaging.



Legal (internal and outside counsel)
Analyze incident for potential reporting obligations and required mitigation.
Messaging – internal and external.
Documentation. Preserve privilege.

Incident Response/Forensics
Contain the incident. Stop data loss.
Preserve evidence. Threat hunting.

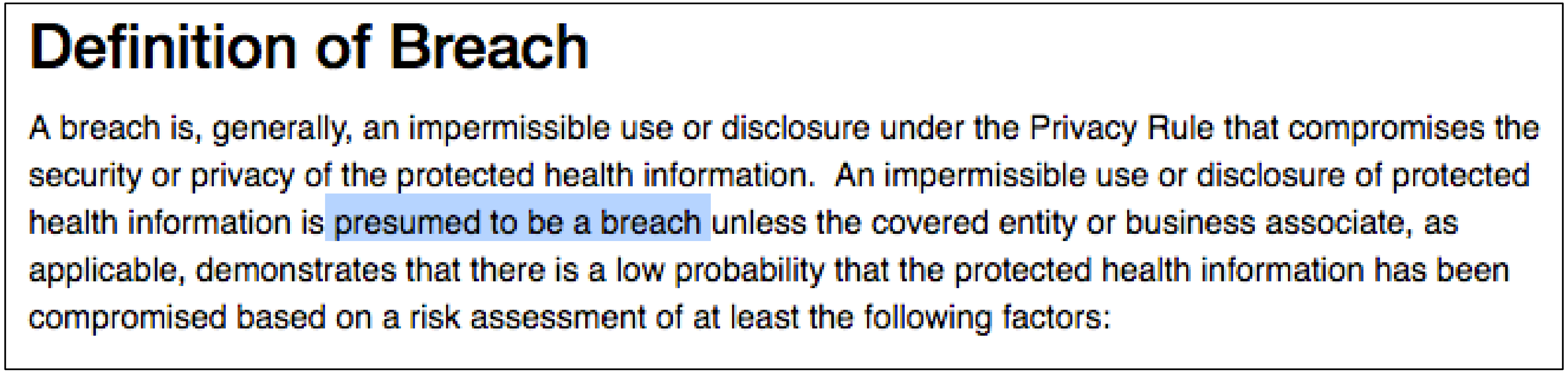
Law Enforcement
Criminal prosecution.

Insurance Carrier
Coverage. Limit spend on legal, IR, penalties, regulatory response.

Public Relations
External messaging / media.

Evaluate Risk of Data Exfiltration

- Do not call incident a breach until counsel determines you have a breach
  - Data exfoliation analysis is needed for legal determination
- Is this incident reportable?
  - HIPAA – presumption of breach (see below)
  - FERPA – release or access
  - States – access vs. acquisition



Definition of Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

Incident Response Analysis

- Consider full scope of applicable laws
  - Review relevant exceptions. For example:
    - Risk of harm
    - Subject to vs. in compliance with HIPAA/FERPA
    - Encryption
    - Paper vs. electronic data
  - Multiple laws may apply
- Separate analysis for each type of affected data
  - Employee data (PI)
  - Student data (PI, education record, treatment record)
  - Patient data (PHI/sensitive data)
  - Non-exfiltrated encrypted PI/PHI
- Contractual notification obligations

Breach Notification

- Individual notification – take into account all applicable laws
  - HIPAA has content requirements
  - State breach notification laws have content, formatting, and credit monitoring requirements
  - Do not play hide the ball with affected individuals
  - What vendors do you need?
    - Credit monitoring – required or best practice?
    - Mailing vendor – undeliverables and substitute notice
    - Call center – script and escalation path
- Media notification
  - Applicable notification laws determine content and distribution
  - Carefully construct notification. This is a piece of evidence against you later.
  - How will you respond to media inquiries?

Breach Notification

- Regulator notification
  - Managing timing
  - Control the messaging when possible – narrative vs. portal notification
  - OCR breach notification
  - Consistent messaging
- Other notification obligations
  - PCI
  - Contracts
  - Credit monitoring agencies

Thank you. Questions?

Meghan O'Connor
meghan.oconnor@quarles.com
(414) 277-5423

© 2021 Quarles & Brady LLP - This document provides information of a general nature. None of the information contained herein is intended as legal advice or opinion relative to specific matters, facts, situations or issues. Additional facts and information or future developments may affect the subjects addressed in this document. You should consult with a lawyer about your particular circumstances before acting on any of this information because it may not be applicable to you or your situation.