Campus Cybersecurity-A Practical Approach To Implementation

CSEPN Annual Conference

August 18, 2021

Brandon Sherman and Sarah Glover

MAYNARD COOPER GALE

OUR **CLIENT BASE**

KEY INDUSTRIES SERVED

- Admiralty and Maritime
- Automotive and Aerospace
- Agriculture
- Autonomy and Robotics Systems
- Banking and Financial Services
- Defense and Aviation
- Energy, Utilities, and Natural Resources
- Fintech
- Governmental Entities
- Health Care
- Higher Education
- Industrial, Manufacturing, and Distribution
- Insurance
- Internet of Things (IoT)
- Life Sciences
- Manufacturing
- Medical Devices
- Non-Profit
- Outdoor Products
- Personalized Medicine and Genomics
- Real Estate
- Senior Living and Long-Term Care
- Sports and Entertainment

MAYNARD
COOPER GALE

TWELVE OFFICES **COAST TO COAST**

6

NEW MAJOR MARKETS
LAST FIVE YEARS

MAYNARD
COOPER GALE

HIGHER EDUCATION PRACTICE

- The Higher Education Practice Group is deeply experienced in all manner of regulatory issues that are important to institutions, investors, third-party servicers and accrediting agencies.

Title IV	Accreditation	State Licensure
Cybersecurity	False Claims Act	Title IX
Transactions	Government Relations	Government Investigations

Presenter Background

Brandon Sherman

- Practice and Experience
  - Previous Experience: Senior Counsel to the Deputy Secretary
  - Advises institutions on meeting U.S. Department of Education cybersecurity requirements
  - Counsels clients on the rules and procedures related to federal financial aid, accreditation, Title IX, and transactional issues
- Contact Information
  - Bsherman@MaynardCooper.com
  - 202-868-5925

NATIONALLY RANKED **CYBERSECURITY & PRIVACY PRACTICE**

MAYNARD
COOPER GALE

Presenter Background

Sarah Glover

- Practice and Experience
  - Shareholder, Cybersecurity & Privacy practice group
  - Advises clients on cybersecurity compliance and governance, data breach planning and response, cybersecurity risk assessment, vendor management, and cybersecurity issues in transactions.
  - Adjunct professor of Cybersecurity Law at University of Alabama School of Law
- Contact Information
  - SGlover@MaynardCooper.com
  - 205-254-1877

MAYNARD
COOPER GALE

LEGAL DISCLAIMER

- The purpose of this presentation is to provide news and information on legal and regulatory issues, and all content provided is for informational purposes only. It should not be considered legal advice.
- The transmission of information from this presentation does not establish an attorney-client relationship with the participant or reader. The participant or reader should not act on the information contained in this presentation or any accompanying materials without first consulting retained legal counsel.
- If you desire legal advice for a particular situation, you should consult an attorney.

TOPICS

Current Trends in Cybersecurity

Compliance Landscape

Role of Institutional Leadership

Breach Reporting and Response

Cybersecurity Best Practices

MORE THAN COMPLIANCE

Financial impact

Reputational damages

Litigation risks

Operational disruption

RECENT CYBER TRENDS

- **Ransomware** attacks and **extortion** attacks have been rampant.
- **Business email compromise** schemes continue to plague organizations of all industries.
- Data breach **costs** continue to grow. Average cost of a data breach in 2020 in the education sector was **$3.9M**.

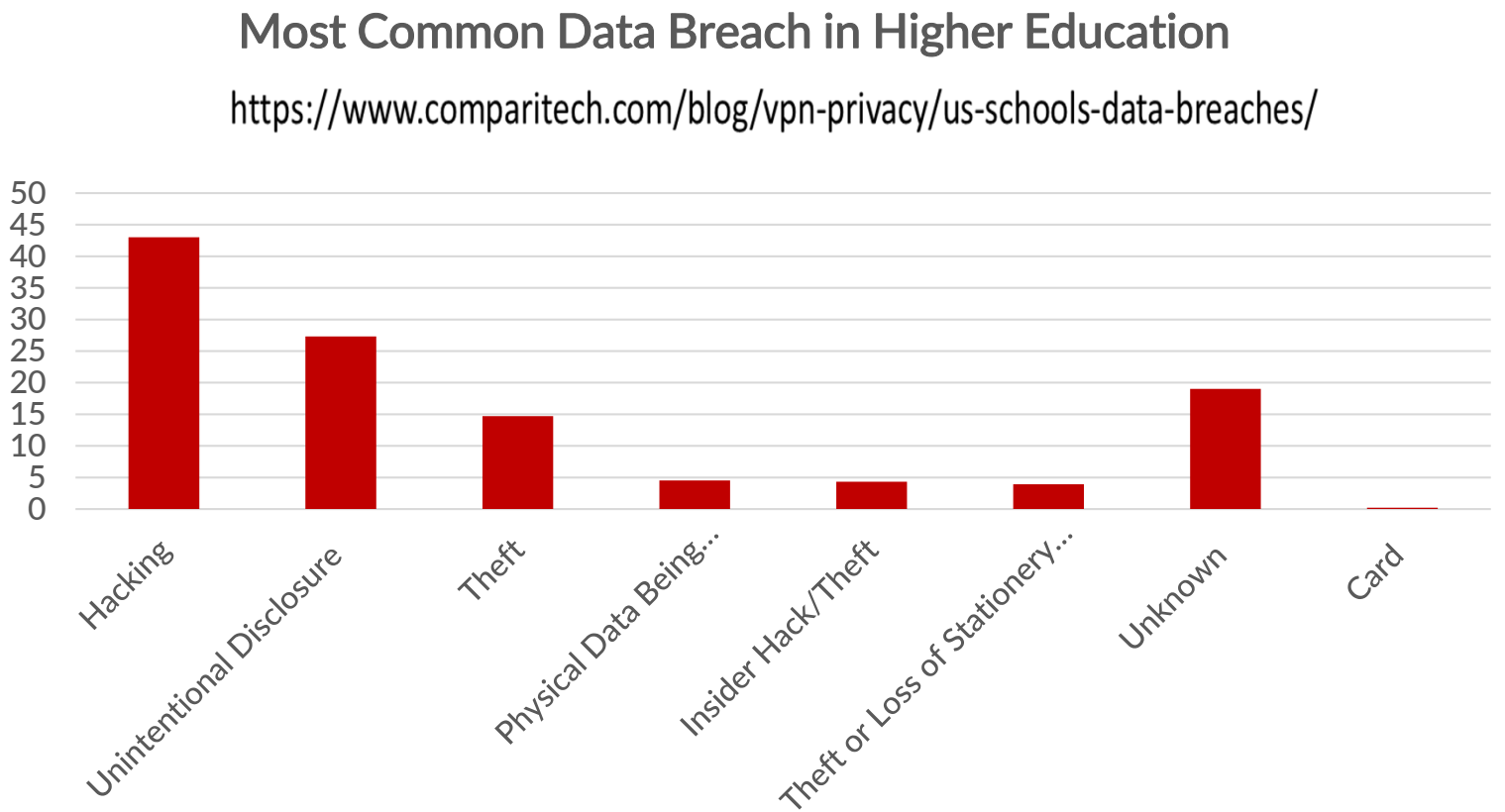
INSTITUTIONS ARE **TARGETED** BY CYBER CRIMINALS

- They collect and store a high volume of **sensitive data** (financial, health, PII).
- The **operational impact** of a cyber attack could be crippling. . . and criminals know this.
- Without critical systems, you may be unable to:
  - Hold classes
  - Process payments
  - Pay employees
  - Process grades
  - Communicate with students and faculty
- Increased vulnerabilities due to **COVID-19**.

COMMON CYBER INCIDENTS

- Target student **PII** to resell on the black market.
- Encrypting school system data for **ransom**.
- Target student **direct deposit information** to redirect financial aid reimbursements to attacker bank accounts.
- IRS impersonation scam that appears to primarily target educational institutions.

BREACH CAUSES



MAYNARD
COOPER GALE

COVID-19

- Prior assumption that everyone is working on campus
- Prioritizing access over security
- Lack of time for training and preparing staff for the remote environment
- Use of personal and unsecure devices
- Working in unsecure locations

U.S. Department of Education Annual Performance Plan

FY 2022 Strategic Goal 3.2

The Department will:

- Continue to refine processes to **actively monitor** cybersecurity compliance and the risk factors associated with performing cybersecurity reviews.
- Work to remediate **Gramm-Leach-Bliley Act** noncompliance in IHEs and work with IHEs to proactively put in place compliance programs.

U.S. Department of Education Annual Performance Plan (cont.)

- Continue to address the requirements to:
  - Address the federal mandate to protect controlled unclassified information that is transmitted, processed, of destroyed IHEs in accordance with **NIST SP 800-171**, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.*
  - Educate, support, and incentivize IHEs to mature their **cybersecurity postures to protect FSA data** and student data more effectively.

CYBERSECURITY/DATA PRIVACY COMPLIANCE

- Gramm-Leach-Bliley Act (GLBA)
- Student Aid Internet Gateway (SAIG)
- Family Educational Rights and Privacy Act (FERPA)
- State privacy and breach notification laws
- NARA CUI Rule/NIST SP 800-171
- HEA data use sharing limitations (20 U.S.C. 1090)

APPLICABLE DEPARTMENT REGULATIONS

Administrative Capability (34 C.F.R. § 668.14)

- To begin and continue participation in Title IV programs, an institution must maintain appropriate institutional capability for the sound administration of Title IV programs.
  - The maintenance of adequate checks and balances in IHEs systems of internal control.

PROGRAM PARTICIPATION AGREEMENT

- Institutions agree to comply with the GLBA, Safeguards Rule.
- Institutions are strongly encouraged to inform its students and the Department of any breach.
- "The Secretary considers any breach to the security of student records and information as a demonstration of a potential lack of administrative capability."

GLBA RULE OVERVIEW

- GLBA-Safeguards Rule (effective 2003)
  - Requires **financial institutions** to ensure the security and confidentiality of this financial of information.
- Postsecondary institutions are considered financial institutions.
- The Safeguards Rule is enforced by the FTC.

GLBA REQUIREMENTS

- Develop, implement, and maintain a **written information security program**;
- Designate the employee(s) responsible for **coordinating** the information security program;
- Periodically **evaluate and update** your school's security program;
- **Identify and assess** risks to customer information; and;
- **Select** appropriate service providers that are capable of maintaining appropriate safeguards.

EXAMPLES OF GLBA NONCOMPLIANCE

- Use of elevated domain privilege administrator accounts that are not password protected. These accounts were widely distributed to staff.
- Scanning and storage of PII to a network that can be easily accessed through any of the common administrator accounts.
- Using a program that captures keystrokes typed on the keyboard (keylogger).

SCHOOL LEADERSHIP RESPONSIBILITIES UNDER GLBA

Presidents and Chief Information Officers should have, at a minimum:

- Evaluated and documented their current security posture against the requirements of GLBA; and
- Have taken immediate action to remediate any identified deficiencies (DCL GEN-16-12).

GLBA AUDIT PROCEDURES

a) Verify that the institution has designated an individual to coordinate the **information security program.**

b) Verify that the institution has performed a **risk assessment** that addresses the three required areas
   - Employee training
   - Information systems
   - Detecting, preventing, and responding to attacks

c) Verify that the institution has documented a **safeguard** for each risk identified from step b above.

MAYNARD
COOPER GALE

AUDIT FINDINGS FOLLOW-UP

FSA's Cybersecurity Team will be informed of the GLBA audit findings and may request additional information to assess the level of risk to student data	Referral to the FTC for enforcement
Develop a corrective action plan	If the Cybersecurity Team determines the institution poses a substantial security threat, it may temporarily or permanently disable the school's access to Department systems
The Cybersecurity Team provides technical assistance to remediate the security threat	Referral to FSA's Administrative Actions and Appeals Service Group for a possible administrative action

SAIG

- Federal Student Aid Application Systems (e.g. COD & NSLDS)
- Must ensure that Title IV data is protected from access by or disclosure to unauthorized personnel
- The SAIG Enrollment Agreement requires schools to **immediately notify** the Department of a breach.
- GLBA compliance requirement
- Institutions' **point of contact** information

BREACH NOTIFICATION

- Must **immediately notify** the Department of a breach or suspected breach. (SAIG agreement)
- How to report a breach:
  - cpssaig@ed.gov
  - Include date of the incident, impact of breach, remediation status
- Keep in mind overlapping state data breach notification laws.

WHAT HAPPENS WHEN I REPORT BREACH?

- FSA Technology Office receives the incident report.
- Report is analyzed & categorized by the Technology Office.
- The Technology Office works with the institution to get a technical understanding of what happened.
- Provides recommendations and best practices to the institution.
- Possible follow-up actions:
  - E.g. ongoing monitoring, referral to the School Participation Division

NIST SP 800-171 OVERVIEW

- The NARA CUI rule establishes that agencies must enter into an agreement with a non-executive branch entity to share CUI and require compliance with the standards set forth in NIST SP 800-171.
- NIST SP 800-171
  - Defines the security requirements (controls) required to protect CUI in nonfederal information systems and organizations (minimum standards).
  - Requirements apply to all components of nonfederal systems **that process, store, and/or transmit CUI**.

SECURITY REQUIREMENT FAMILIES

- Limit information system access to authorized users (Access Control Requirements).
- Ensure that system users are properly trained (Awareness and Training Requirements).
- Create information system audit records (Audit and Accountability Requirements).

SECURITY REQUIREMENT FAMILIES

- Establish baseline configurations and inventories of systems (Configuration Management Requirements).
- Identify and authenticate users appropriately (Identification and Authentication Requirements).
- Establish incident-handling capability (Incident Response Requirements).

SECURITY REQUIREMENT FAMILIES

- Perform appropriate maintenance on information systems (Maintenance Requirements).
- Protect media, both paper and digital, containing sensitive information (Media Protection Requirements).
- Screen individuals prior to authorizing access (Personnel Security Requirements).

SECURITY REQUIREMENT FAMILIES

- Limit physical access to systems (Physical Protection Requirements).
- Conduct risk assessments (Risk Assessment Requirements).
- Assess security controls periodically and implement action plans (Security Assessment Requirements).

SECURITY REQUIREMENT FAMILIES

- Monitor, control, and protect organizational communications (System and Communications Protection Requirements).
- Identify, report, and correct information flaws in a timely manner (System and Information Integrity Requirement).

POSSIBLE COMPLIANCE SOLUTIONS

- Third-party servicers
- Implement alternative, but equally effective, security measures
- FSA practical solutions
- Technical assistance

WHAT OTHER SCHOOLS ARE DOING

- Utilizing third-party servicers
- Consulting with legal counsel and cybersecurity experts, as appropriate
- Assessing for compliance with NIST SP 800-171
- Ensuring sufficient financial and staffing resources are available

SCHOOL LEADERSHIP

- Presidents and Chief Information Officers of institutions should have, at a minimum:
  - Evaluated and documented their current security posture against the requirements of GLBA; and
  - Have taken immediate action to remediate any identified deficiencies.
- Cybersecurity phases
  - Identify, protect, detect, respond, and recover
- Support your school's efforts
- Know your cybersecurity leads

Data Breach Legal Update and Best Practices

MAYNARD
COOPER GALE

COLONIAL PIPELINE LAWSUIT

- A gas station filed a class action complaint in federal district court in Georgia on June 21, 2021 because of the fuel shortages that resulted from the ransomware attack that hit Colonial Pipeline on May 7, 2021.
- The Plaintiffs allege that Colonial failed to take and implement adequate and reasonable measures to ensure that the pipeline's critical infrastructure was safeguarded.

> 23. As discussed below, the nature of Defendant's security lapse for its electronic systems was basic and grossly negligent. It occurred despite advance knowledge and warnings, including prior cybersecurity incidents involving pipelines. In the lead-up to the electronic break-in, Defendant had repeatedly ignored and rejected efforts by the applicable regulatory agency to meet with it so as to check on its cybersecurity. Defendant is a lucrative and well-resourced

COLONIAL PIPELINE LAWSUIT

Key takeaways:

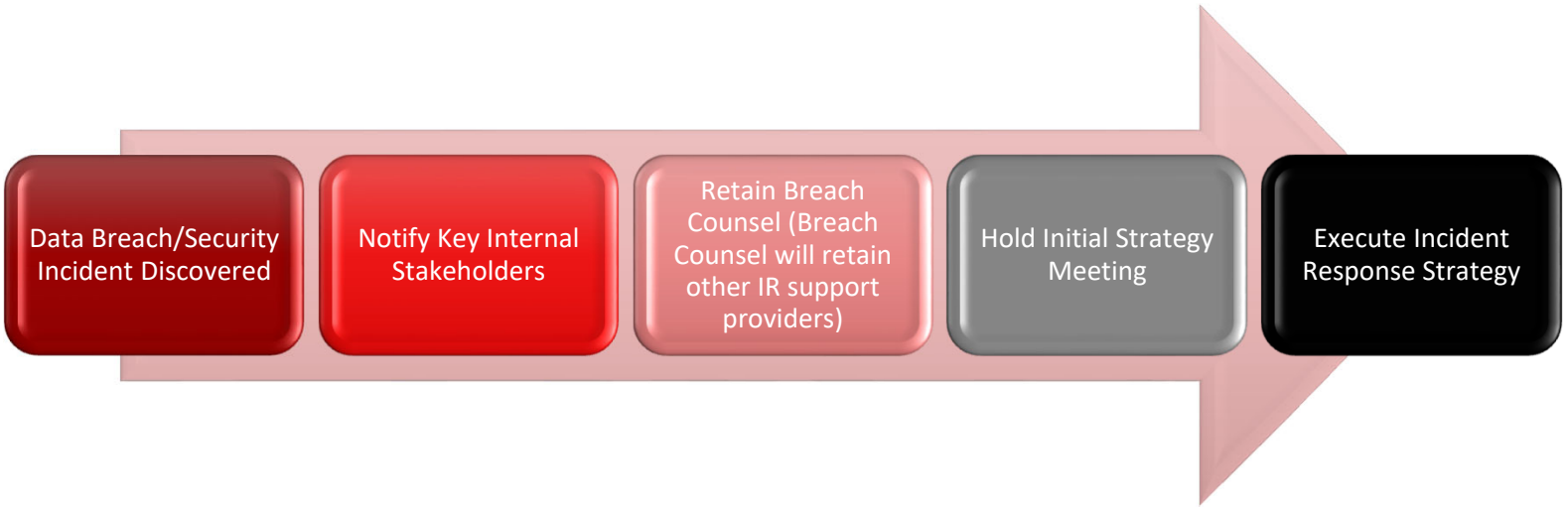
- Failure to have an **incident response plan** in place to address ransomware attacks can lead to legal liability.
- Legacy systems, lack of multi-factor authentication, and unpatched vulnerabilities in VPNs, which all commonly serve as root causes of security attacks, can create **legal exposure**.

systems was minimal. It had no plan in place for ransomware attacks and had left up a legacy VPN system without shutting off logins and passwords for old employees – a basic failure according to Defendant's own later-retained experts.

THREE "WHOS" OF INCIDENT RESPONSE

- Who needs to be involved internally?
- Who is our insurance carrier?
- Who do we need to hire?

INCIDENT RESPONSE ROADMAP – First Steps



INCIDENT RESPONSE ROADMAP – First Steps

- **DO** Engage Legal Counsel
- **DO** Begin Preservation
- **DON'T** Remediate, Wipe, or Delete Affected Systems or Applications
- **DON'T** Discuss the Incident with Third Parties Without Consulting Legal Counsel
- **DO** Disconnect Machines From the Network. **DON'T** Power Them Off.

FAILURE TO TIMELY ENGAGE LEGAL COUNSEL COULD RESULT IN:

1. Losing the protection of the attorney-client privilege.
2. Missing statutory notice deadlines or legal reporting obligations.
3. Losing key forensic evidence.
4. Saying the wrong things to external audiences.
5. Unintentionally misrepresenting what happened (over/under selling).
6. Not assembling the right team.

MAYNARD COOPER GALE

Intentional steps must be taken to preserve the privilege

MAYNARD
COOPER GALE

CAPITAL ONE DECISION

- June 2020: Federal district court in VA orders Capital One to **disclose a forensic investigation report** to the plaintiffs in a lawsuit stemming from Capital One's 2019 data breach because:
  1. Capital One and Mandiant entered into a **non-privileged** SOW.
  2. Post-breach SOW included **same scope of work** as non-privileged, pre-breach SOW.
  3. Forensic report was **widely distributed**.
- **Not enough** to maintain privilege:
  - Mandiant's work was performed at the direction of counsel.
  - Final report was initially delivered to outside counsel.

RUTTER'S DECISION

- July 2021: Federal district court in PA orders Rutter's to **disclose a forensic investigation report** prepared by Kroll to the plaintiffs in a data breach lawsuit against the gas station and convenience store chain.
- The Court found the report was **NOT privileged** because:
  1. it was "clear from the contract between Kroll and defendant that the primary motivating purpose behind the Kroll report was not to prepare for the prospect of litigation."
  2. The purpose of the investigation, as stated in the SOW, was to determine *whether* data was compromised, and the scope of such compromise *if it occurred.*
  3. Without knowing whether or not a data breach had occurred, defendant cannot be said to have unilaterally believed that litigation would result.

Of course, the best kind of data breach. . .

is the one that never happens.

MAYNARD
COOPER GALE

CYBERSECURITY QUICK **WINS**

- Cybersecurity awareness **training**
- Lock down your **email** environment
- Review **record retention** policies
- Evaluate key **vendors** with access to sensitive data

MAYNARD
COOPER GALE

WHAT'S NEXT?

- Proposed changes to GLBA
- FSA enforcement activity
- IRS/Protecting taxpayer information
- Changes to the annual compliance audit
- Stakeholder engagement

RESOURCES

- Dear Colleague Letters: GEN 16-12 & GEN 15-18
- Electronic Announcement
  - *Enforcement of Cybersecurity Requirements under the Gramm-Leach-Bliley Act* (February 2020)
- FSA Handbook
- NIST SP 800-171
- US-CERT

QUESTIONS?

Presenters:

Brandon S. Sherman
BSherman@maynardcooper.com
202.868.5925

Sarah S. Glover
SGlover@maynardcooper.com
205.254.1877

MAYNARD
COOPER GALE

THANK YOU