Cybersecurity and Data Protection Issues

FAPSC Annual Conference

August 5, 2021

Brandon Sherman & Roger Swartzwelder

MAYNARD COOPER GALE

PRESENTER BACKGROUND

Roger Swartzwelder

- Practice and Experience
  - Shareholder, Higher Education Group
  - Former 13-year General Counsel and Chief Compliance Officer of national career college chain
  - Former national accrediting agency commissioner and senior executive
- Contact Information
  - RSwartzwelder@MaynardCooper.com
  - (202) 868-5929

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

MAYNARD
COOPER GALE

TWELVE OFFICES **COAST TO COAST**

6

NEW MAJOR MARKETS
LAST FIVE YEARS

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

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

NATIONALLY RANKED **CYBERSECURITY & PRIVACY PRACTICE**

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

Evolving Trends in Cybersecurity

Compliance Landscape

Breaching Reporting and Response

Role of Institutional Leadership

Cybersecurity Best Practices

THREATS TO DATA

- 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.

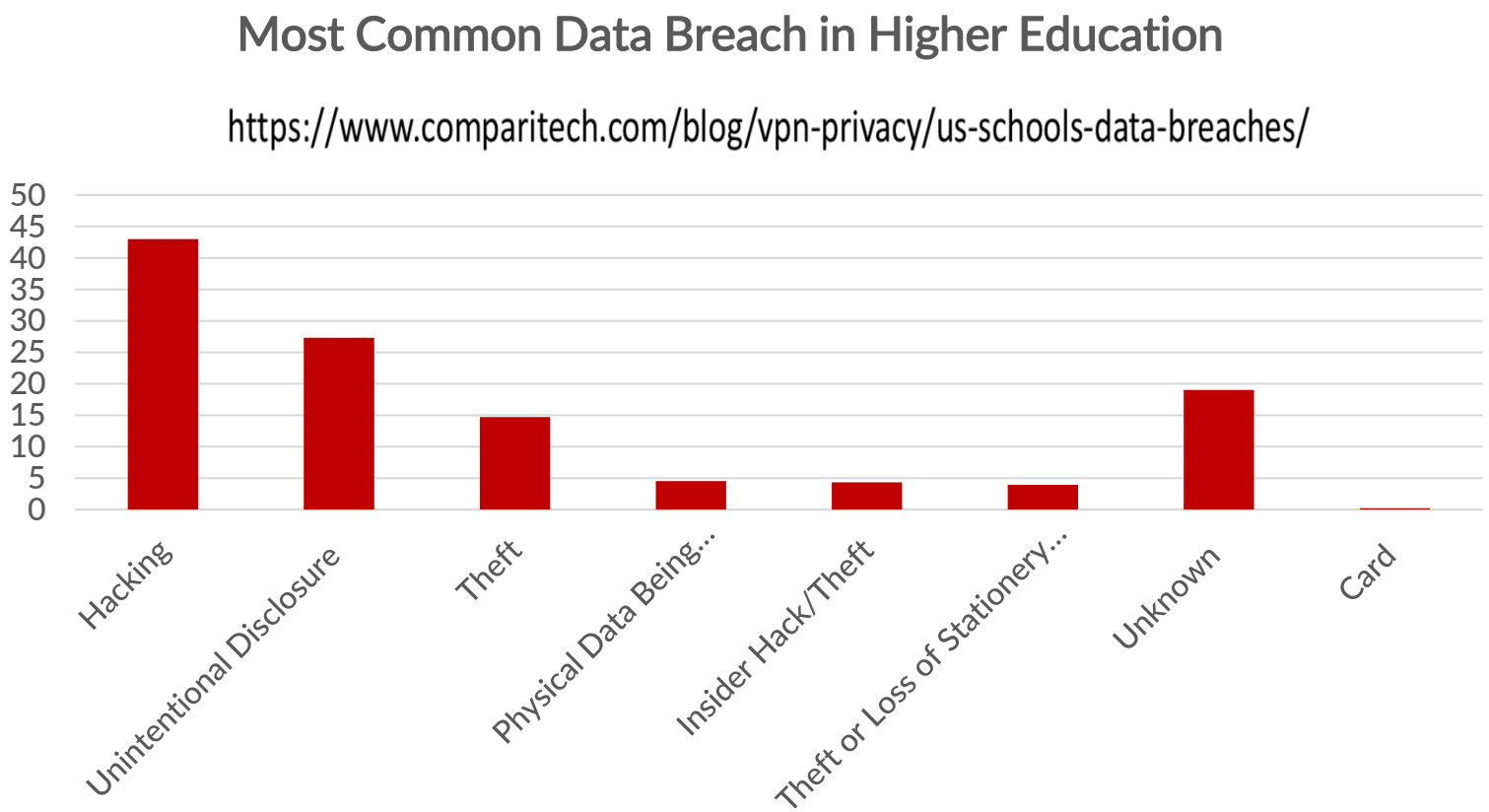
CYBER **TRENDS**

- Ransomware attacks and extortion attacks have been rampant.
  - Ransomware attacks against universities increased by 100% between 2019 and 2020. (BlueVoyant)
- Ever-increasing reliance on mobile devices, remote learning, and third-party education partners is multiplying the higher education attack surface.
- Data breach costs continue to grow. Average cost of a data breach in 2020 in the education sector was $447,000. (BlueVoyant)

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
- Working in unsecure locations
- More stringent budget cuts

BREACH CAUSES



MAYNARD
COOPER GALE

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 **GLBA** noncompliance in IHEs and work with IHEs to proactively put in place compliance programs.

U.S. DEPARTMENT OF EDUCATION **ANNUAL PERFORMANCE PLAN** (CONT'D)

- Continue to address the requirements to:
  - Address the federal mandate to protect controlled unclassified information (CUI) 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
- General Data Protection Regulation (GDPR)
- NARA CUI Rule/NIST SP 800-171

STATUTORY AUTHORITY

Section 143(e) of the Higher Education Act

- Any entity that maintains or transmits information under a transaction covered by this section shall maintain **reasonable and appropriate administrative, technical, and physical safeguards**—

  1. to ensure the integrity and confidentiality of the information; and

  2. to protect against any reasonably anticipated security threats, or unauthorized uses or disclosures of the information.

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 (16 C.F.R. Part 314)
  - Requires **financial institutions** to ensure the security and confidentiality of customer financial 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).

CYBERSECURITY **NON-COMPLIANCE**

- Loss of access to FSA systems
- Initiation of a **Termination Action**
- Denial of an Open Recertification Action
- Initiation of a Limitation Action
- Imposition of a Fine action
- Placement on **HCM**

GLBA **AUDIT REQUIREMENT**

- Added to the Compliance Supplement and **OIG Audit Guide** in 2019
- GLBA light
- Doesn't test for effectiveness

MAYNARD
COOPER GALE

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**

- Definition of a breach: OMB M-17-12
- How to report a breach:
  - cpssaig@ed.gov
  - Include date of the incident, method of breach, 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

BREACH NOTIFICATION **BEST PRACTICES**

- Don’t wait to report!
  - Department is generally aware of unreported breaches.
- Seek advise from counsel.
- Ensure school leadership is involved in the process.

OFFICE OF **INSPECTOR GENERAL**

- Independent component of the U.S. Department of Education.
- Considered a law enforcement agency (subpoena and arrest authority).
- Investigate crimes and criminal cyber threats against:
  - Jurisdiction over criminal activity in cyber space that threatens the Department's administration of Title IV funds.
- Focused on catching the bad guys.

OFFICE OF **INSPECTOR GENERAL** (CONT'D)

- If FSA suspects criminal activity, the incident is referred to OIG.
- In regular communications with FSA.
- Refer to the DOJ for possible prosecution.
- Conducts independent audits and other reviews.

DECEMBER 2020 **ELECTRONIC ANNOUNCEMENT**

- Announcement of the **Campus Cybersecurity Program**
- Informed IHEs & third-party servicers about upcoming activities to ensure compliance with the National Institute of Standards and Technology, Rev. 2, *Controlled Unclassified Information in Non-Federal Systems* (NIST SP 800-171)
- Reminder of continuing obligations to comply with GLBA and the SAIG agreement
- NIST SP 800-171 self-assessment
- Additional information forthcoming in 2021

NIST SP 800-171 BACKGROUND

- Executive Order 13556
- NARA CUI rule (32 C.F.R. Part 2000)
  - Controlled Unclassified Information (CUI) is information the federal government **creates or possesses** and that a law, regulation, or federal government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls
  - Agreement requirement

NIST SP 800-171 **BACKGROUND**

- To provide federal agencies with recommended requirements for protecting the confidentiality of CUI.
- Applies to components of nonfederal systems that process, store, or transmit.
- Colleges are nonfederal organizations that maintain/transmit nonfederal information.

EXAMPLES OF **CUI**

Student financial information	Student Records
Military Records	Personally Identifiable Information

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** (CONT'D)

- 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** (CONT'D)

- 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** (CONT'D)

- 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** (CONT'D)

- 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).

The best kind of data breach. . .

is the one that never happens.

MAYNARD
COOPER GALE

CYBERSECURITY **QUICK WINS**

- Implement multi-factor authentication
- Implement cybersecurity awareness training
- Mandate that all sensitive information will be password protected
- Install a robust anti-virus program
- Restrict access

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. (DCL GEN-16-12)
- Cybersecurity phases
  - Identify, protect, detect, respond, and recover
- Support your school's efforts
- Know your cybersecurity leads

LONG TERM CYBERSECURITY STRATEGIC **GOALS**

- Review and risk-rank your vendors who have access to sensitive data.
- Establish top-down approach to cybersecurity risk management.
- Engage independent third party to perform holistic risk assessment.

MAYNARD
COOPER GALE

WHAT'S **NEXT?**

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

RESOURCES

- Dear Colleague Letters: GEN 16-12 , GEN 15-18
- Electronic Announcement: Protecting Student Information – Compliance with CUI and GLBA
- FSA Handbook
- NIST SP 800-171
- US-CERT

QUESTIONS?

Presenters

Brandon S. Sherman
BSherman@maynardcooper.com
202.868.5925

Roger Swartzwelder
RSwartzwelder@maynardcooper.com
202.868.5929

MAYNARD
COOPER GALE

THANK YOU