Campus Cybersecurity: The Path Forward

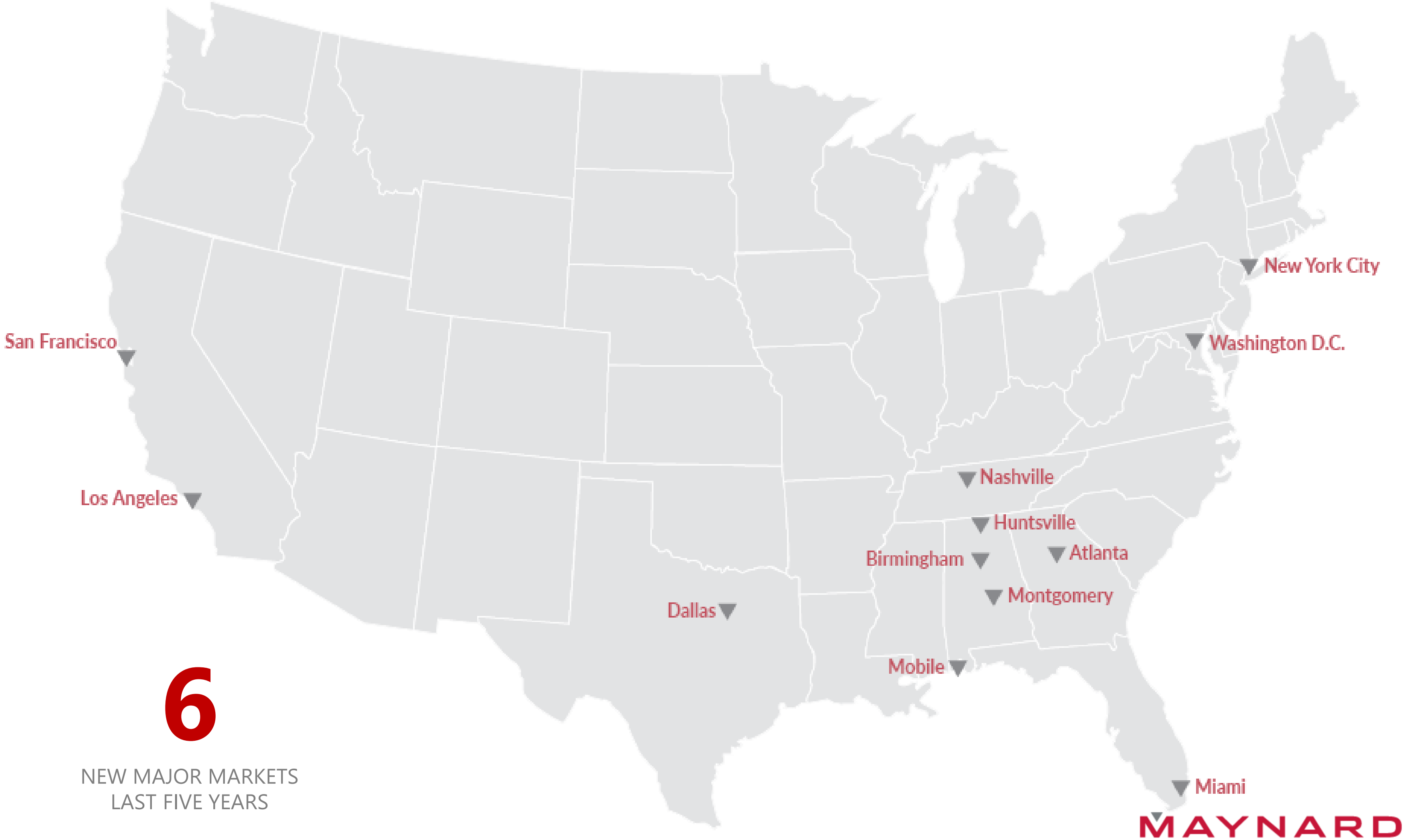
Brandon Sherman & Sarah Glover

May 26, 2021

DEAC Webinar

MAYNARD
COOPER GALE

TWELVE OFFICES **COAST TO COAST**



6

NEW MAJOR MARKETS
LAST FIVE YEARS

MAYNARD
COOPER GALE

OUR **CLIENT BASE**

3 BY AIRBUS

BlueCross BlueShield of Alabama

NEW YORK LIFE

REGIONS

AIG

MassMutual FINANCIAL GROUP

McWANE

Protective.

Sempra Energy

KINDER MORGAN INC

USS

airbnb

Cigna.

Square

THE HARTFORD

JPMorganChase

MetLife

RAYMOND JAMES

Nationwide

Clayton homes

USAA

elpaso

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

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.

PRESENTER BACKGROUND

Brandon Sherman

- Practice and Experience
  - Former U.S. Department of Education official
  - 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

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

TOPICS

Overview of Cybersecurity and Data Privacy Requirements and Risks

Update from the Department of Education

Cybersecurity Best Practices

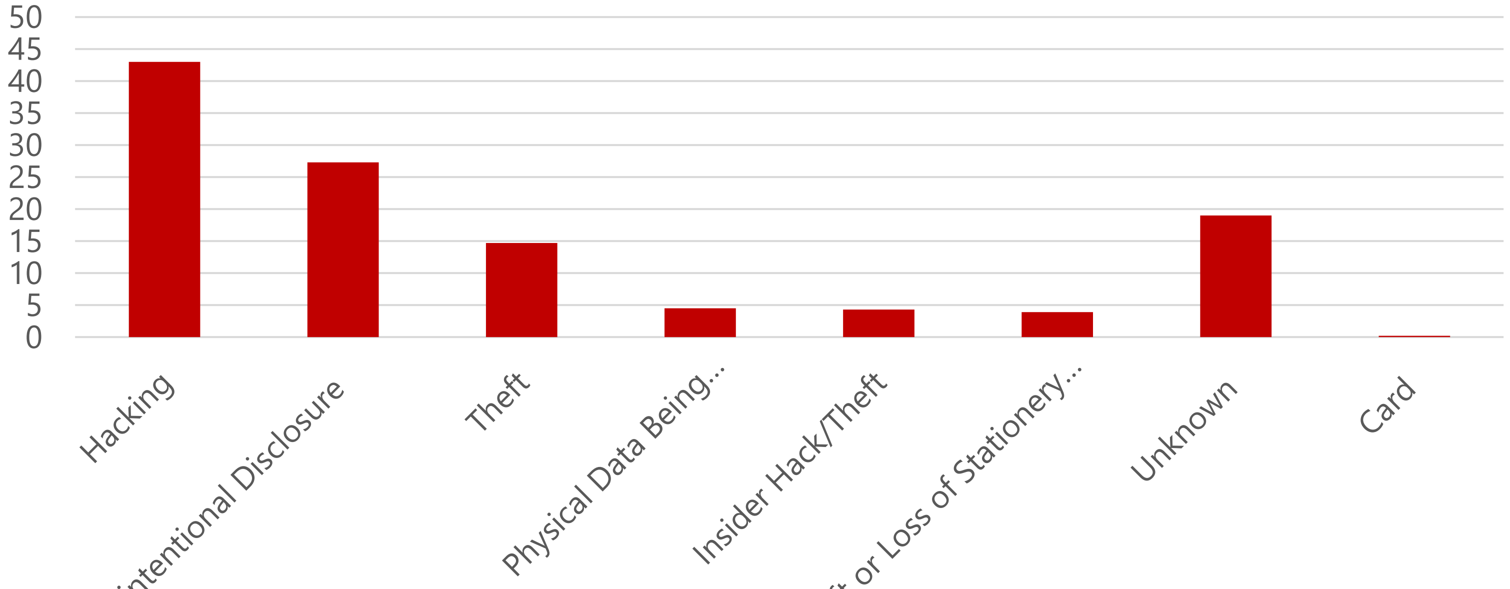
WHY ARE HIGHER EDUCATION INSTITUTIONS TARGETED IN CYBER ATTACKS?

- 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.
- Ransomware attacks are on the rise
- Increased vulnerabilities due to COVID-19

```
        _VER > 1000
#pragma once
#endif // _MSC_VER > 1000
#ifndef __AFXWIN_H__
        #error include
#endif
#include "resource.h"
// CDMotionApp:
// See DMotion.cpp for the
//
class CDMotionApp : public
{
public:
        CDMotionApp();
// Overrides
        // ClassWizard
        //{{AFX_VIRTUAL(
        public:
        virtual BOOL
        //}}AFX_VIRTUAL
// Implementation
        //{{AFX_MSG(
        afx_msg void
                // NOTE
                //    DO NOT
```

BREACH CAUSES

Most Common Data Breach in Higher Education



https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/

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

COMPLIANCE REQUIREMENTS

- Gramm-Leach-Bliley Act (GLBA)
- Student Aid Enrollment Agreement (SAIG)
- Family Educational Rights and Privacy Act (FERPA)
- State privacy and breach notification laws
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPPA)

MORE THAN COMPLIANCE

Financial impact

Reputational damages

Litigation risks

Operational difficulties

SCOPE OF INFORMATION

- Title IV Data: **Student financial information and PII** used in the administration of Title IV Federal student aid programs
    - Examples: Student and parent demographic and financial information submitted on the FAFSA and student-level award grant and loan data
- Who has the student financial information?
- Who is responsible for protecting Title IV data?

DEPARTMENT'S 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 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

Gramm-Leach-Bliley Act (GLBA) was enacted in 1999 (Pub. L. No. 106-102)

GLBA requires financial institutions to provide customers with information about the institutions' privacy practices and about their opt-out rights, and to implement security safeguards.

Subtitle A of Title V of the GLBA requires the FTC to issue regulations requiring financial institutions to develop standards relating to physical safeguards for certain information.

GLBA OVERVIEW

- GLBA (Safeguards Rule) was enacted in 2003 (16 C.F.R. Part 314)
- The Safeguards Rule is enforced by the **FTC**
- **Most postsecondary institutions** are considered financial institutions 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.

SCHOOL LEADERSHIP RESPONSIBILITIES UNDER GLBA

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)

EXAMPLES OF INSTITUTIONS 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)

GLBA AUDIT REQUIREMENT

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

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

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
  - Definition of a breach: OMB M-17-12:
    - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where
      1. a person other than an authorized user accesses or potentially accesses personally identifiable information or
      2. an authorized user accesses or potentially accesses personally identifiable information other than for an authorized purpose.
- GLBA compliance requirement
- Institutions' **point of contact** information

ENFORCEMENT

- U.S. Department of Education
  - Subpart G actions (termination, suspension, fines) (34 C.F.R. Subpart G)
  - Loss of access to Department system
  - Heightened Cash Monitoring (HCM)
  - Warning letter

- Office of Inspector General

- FTC
  - Fines
  - Independent validation
  - Reporting requirements

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

National Institute of Standards and Technology
U.S. Department of Commerce

- 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 PURPOSE

- When the CUI is resident in **nonfederal information systems and organizations**
- To provide federal agencies with recommended requirements for protecting the confidentiality of CUI
- Where the CUI does not have specific safeguarding requirements prescribed by the authorizing law, regulation, or governmentwide policy. When the information systems **where the CUI resides are not operated by organizations** on behalf of the federal government

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); and
- Identify, report, and correct information flaws in a timely manner (System and Information Integrity Requirement).

POSSIBLE COMPLIANCE SOLUTION

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

IMPLEMENTATION

- Review self-assessments
- Establish security controls
- Phased in implementation
- Provide additional guidance

The best kind of data breach. . .

is the one that never happens.

MAYNARD
COOPER GALE

TO PROTECT DATA. . .

You must know where it lives.

You must assign someone to protect it.

You must establish, fund, and support data protection measures.

CYBERSECURITY QUICK WINS

- Written incident response plan
- Cybersecurity awareness training
- Review cybersecurity insurance coverage
- Lock down your email environment
- Review record retention policies

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

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

QUESTIONS?

Contact Information

Brandon S. Sherman
BSherman@maynardcooper.com
202.868.5925

Sarah S. Glover
SGlover@maynardcooper.com
205.254.1877

THANK YOU

MAYNARD
COOPER GALE