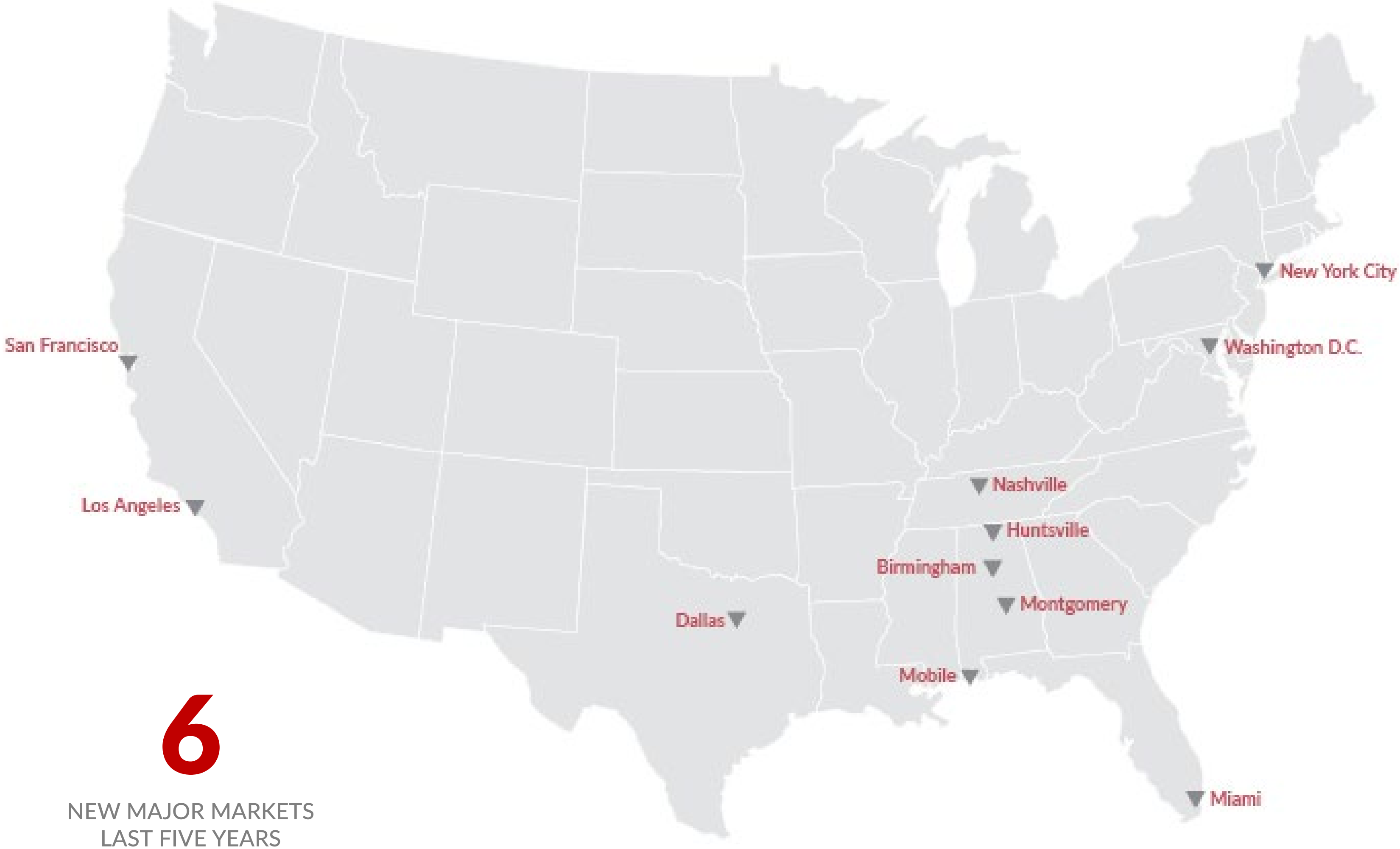
Campus Cybersecurity: The Path Forward

March 17, 2021

MAYNARD
COOPER GALE

ELEVEN 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

TOPICS

Overview of Cybersecurity and Privacy Requirements and Risks

Update from the Department of Education

Overview of NIST SP 800-171

INFORMATION SECURITY AT IHES

- Gramm-Leach-Bliley Act (GLBA)
- 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

CYBERSECURITY THREATS TO YOUR DATA

- Volume of financial information and PII
- Ransomware attacks are on the rise
- Increased vulnerabilities due to COVID-19

```
[illegible]_VER > 1000
#pragma once
#endif // _MSC_VER > 1000
#ifndef __AFXWIN_H__
        #error include [illegible]
#endif
#include "resource.h"       // [illegible]
// CDMotionApp:
// See DMotion.cpp for the [illegible]
//
class CDMotionApp : public [illegible]
{
public:
        CDMotionApp();
// Overrides
        // ClassWizard [illegible]
        //{{AFX_VIRTUAL([illegible]
        public:
        virtual BOOL [illegible]
        //}}AFX_VIRTUAL

// Implementation
        //{{AFX_MSG(CD[illegible]
        afx_msg void On[illegible]
                // NOTE - the [illegible]
                //    DO NOT [illegible]
                //}}AFX_MSG [illegible]
```

DATA BREACH STATISTICS

- Data breaches exposed 36 billion records in the first half of 2020.
- Global average cost of a data breach in 2020 in the Education sector was $3.9M.
- Remote working increases the average cost of a data breach by $137K.

SCOPE

- 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?

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.

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
    - "The Secretary considers any breach to the security of student records and information as a demonstration of a potential lack of administrative capability" (PPA)

GLBA

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.

SAFEGUARDS RULE OVERVIEW

- Safeguards Rule (effective in 2003)
- Postsecondary institutions are considered financial institutions by the Federal Trade Commission (FTC)
- The Safeguards Rule is enforced by the FTC
- No changes have been made to the rule

FEDERAL TRADE COMMISSION ★ UNITED STATES OF AMERICA ★ MCMXV

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)

GLBA AUDIT REQUIREMENT

- Compliance Supplement and OIG Audit Guide
- Added in 2019
- GLBA Light
- Determine whether the institution designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 C.F.R. § 314.4 (b); and documented safeguards for identified risks

* Presidents and Chief Information Officers should have 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)

SAIG

- Student Aid Internet Gateway (SAIG)
- Federal Student Aid Application Systems
- 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 for an other than authorized purpose.
- GLBA compliance requirement

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

POLICY DEVELOPMENT

- Agency Priority Goal
- Rulemaking not required
- Legal, policy, technical, and enforcement perspectives
- Stakeholder meetings
- Other options considered
  - Agreement & rulemaking

NIST SP 800-171 BACKGROUND

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

NIST SP 800-171 OVERVIEW

- 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
- Currently: The Department strongly encourages those institutions that fall short of NIST standards to assess their current gaps and immediately begin to design and implement plans in order to close those gaps using the NIST standards as a model (DCL GEN 16-12)

EXAMPLES OF CUI

Student financial information	**Student Records**
Military Records	Personally Identifiable Information (PII)

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).

SELF-ASSESSMENT

- Fall 2021
- Effort to understand IHE readiness to comply with NIST SP 800-171
- Will help ED determine the cybersecurity posture, maturity, and future compliance with NISP 800-171
- Will provide information for the Department to consider potential burdens

IMPLEMENTATION

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

POLICY CHANGES?

- Continuing on schedule
- Federal CUI requirement
- Resources
- Reorganization
- Obama administration & cybersecurity enforcement

POSSIBLE COMPLIANCE SOLUTION

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

ENFORCEMENT

- Subpart G actions (termination, suspension, fines)
- HCM
- Warning letter
- Loss of access to Department systems

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
  - https://ifap.ed.gov/sites/default/files/attachments/2020-01/1920FSAHbkVol2Ch7.pdf
- NIST SP 800-171
  - https://www.nist.gov/publications/protecting-controlled-unclassified-information-nonfederal-information-systems-and-0?pub_id=918804

CYBERSECURITY QUICK WINS

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

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

Presenters:

Brandon S. Sherman
BSherman@maynardcooper.com
202.868.5925

Sarah S. Glover
SGlover@maynardcooper.com
205.254.1877

DISCLAIMER

Please note that the purpose of this presentation is to provide information on legal issues and all content provided is for informational purposes only and should not be considered legal advice.

The transmission of information from this presentation does not establish an attorney-client relationship with the participant. If you desire legal advice for a particular situation, you should consult an attorney

THANK YOU