The Challenges Facing FAA’s

Dan Commons

U.S. Department of Education

2020 Virtual FSA Training Conference for Financial Aid Professionals
AGENDA

01  Cybersecurity Overview
02  The Problem
03  Cybersecurity Guidance
04  Cybersecurity Hygiene
OVERVIEW
WHY ARE WE HERE

• Discuss the challenges that we face together.

• Look at cybersecurity threats.

• Discuss how each one of us plays a role in cybersecurity.

• Understand cybersecurity compliance requirements.
FROM THE HEADLINES

Equinix Data Center Giant Hit By Netwalker Ransomware, $4.5M Ransom

University Pays $457,000 to Ransomware Gang

College Hit With Ransomware Attack; Multiple Systems Impacted
CYBERSECURITY OVERVIEW

• Securing credentials and access controls is more important now than ever as 8.5 billion records were breached in 2019, giving attackers access to more stolen credentials.

• 150,000 vulnerabilities disclosed to date. Patching vulnerabilities is still a problem for many organizations and cybercriminals know that.

• Ransomware attacks up 67% year-over-year in Q4 2019. Threat actors are innovating with new ransomware code for destructive attacks.

• North America the biggest geographic target. Asia, Europe, the Middle East and South America trailed North America in number of attacks.

Data source: https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/
EDUCATION BREACHES

• Public institutions account for 78 percent of education breaches - Overall, 77.7 percent of the breaches occurred in a public school or college. Of these public breaches, 67.7 percent affected colleges. Private colleges were also heavily impacted, accounting for 90.9 percent of all breaches within private institutions.

• The public education breaches affected 20.6 million records, around 20,000 records per breach, in public institutions. Private institution breaches affected 3.9 million records, or around 14,000 records per breach.

Data source: https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/
DEPARTMENT PRIORITY

• Department and FSA Strategic Goals drive the focus.

• Two main focus areas:
  1. Improve student privacy data and cybersecurity controls of IHEs through outreach and communication to mitigate future cyber incidents and breaches.
  2. Strengthen Data Protection and Cybersecurity Safeguards.
THE PROBLEM
OOPS!!!

Your Personal files are encrypted!

Your personal files encryption produced on this computer: photos, videos, documents, etc. Encryption was produced using a unique public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 1.00 bitcoin (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click “Pay with Bitcoin” To open a list of encoded files, click “Show files”

Do not delete this list, it will be used for decryption. And do not move your files.
Evolving Threat Landscape

- Ransomware
- Phishing
- Distance Learning
- Mobile
THREATS TARGETING EDUCATION SECTOR

- Target student direct deposit information to redirect financial aid reimbursements to attacker bank accounts.
- Target student PII for resell on black market.
- Encrypting school systems for ransom.
- Targeting university research and intellectual property.
THREATS TARGETING EDUCATION SECTOR

Significant uptick in ransomware attacks across the nation and the education sector.

Sophisticated credential-theft (username and password) attacks as a vehicle to compromise staff and student banking information.

Compromise of unsecured cloud databases containing sensitive student information.
RANSOMWARE – THE WHAT

• Schools have reported that attackers are targeting their institutions with ransomware. In some institutions successful attacks have caused the school to lose access to their critical systems and data, impacting their ability to operate.

• Phishing attacks are back in favor to gain access to account credentials that the attackers then use to install and propagate ransomware across a network.
RANSOMWARE – THE WHY

- Schools appear to be easy targets:
  - Small IT staffs with limited cybersecurity expertise.
  - Networks designed for open sharing and “academic freedom”.
  - “Trusting” culture with a wide range of external partners.
- The dollars - As financial institutions, they are an attractive target for criminals looking for a lucrative payout.
- The data - Large repositories of personal information.
- The “new world” as a response to COVID-19.
  - Rapid and often minimally secured transition to a remote student population.
  - New technology to facilitate the new paradigm of remote student services.
CYBERSECURITY GUIDANCE
TOPIC AREAS

• Breaches.

• Gramm-Leach-Bliley Act (GLBA).

• National Institute of Standards and Technology (NIST) SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
WHAT IS 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.”

A “data breach” is “the unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.”

For Post-Secondary Institutions the data set is information obtained under or through the Title IV participation agreements.
FSA BREACH PROCESS

01 FSA Team Receives Incident Report

02 FSA Team Collaborates Works with the school to triage and respond to the incident

03 FSA Team Provides Recommendations

04 FSA Team Gathers Lessons Learned

05 FSA Team Shares Best Practices with Schools

Analyzes Trends
HOW TO REPORT A BREACH TO FSA

SEND AN EMAIL

1. To... FSASchoolCyberSafety@ed.gov; cpssaiq@ed.gov
   Cc... Your data breach team, executives, etc. per your policy

Or CALL THE EDUCATION SECURITY OPERATIONS CENTER

(EDSOC) at 202-245-6550 (24 hours a day)

2. INCLUDE THE FOLLOWING INFORMATION
   • Date of breach (suspected or known)
   • Impact of breach (# of records, etc.)
   • Method of breach (hack, accidental disclosure, etc.)
   • Information Security Program Point of Contact (email and phone)
   • Remediation Status (complete, in process – with detail)
   • Next steps (as needed)

3. The school shall report to FSA as they discover the breach so that FSA can work collaboratively with the IHE to resolve the incident
GRAMM-LEACH-BLILEY ACT (GLBA) BACKGROUND

• GLBA was enacted in 1999 (Pub. L. No. 106-102)
  • Provides a framework for regulating the privacy and data security practices of a broad range of financial institutions.
  • Requires financial institutions to provide customers with information about the institutions’ privacy practices and about their opt-out rights, and to implement security safeguards.

• 2019 added Compliance Supplement and OIG Audit Guide
  • Audit Objectives - Determine whether the institution designated an individual to coordinate the information security program; performed a risk assessment; and documented safeguards for identified risks.
GENERAL GLBA REQUIREMENTS

• Develop, implement, and maintain a written information security program.
  • Design and implement an information safeguards program.
  • Select appropriate service providers that are capable of maintaining appropriate safeguards.

• Designate the employee(s) responsible for coordinating the information security program.

• Identify and assess risks to customer information.
  • Periodically evaluate and update your school’s security program.
AGREEMENTS

• Program Participation Agreement (PPA)

Schools must protect student financial aid information, with particular attention to information provided to institutions by the Department or otherwise obtained in the support of the administration of federal student aid programs.

• Student Aid Internet Gateway (SAIG) Agreement

Agreement includes a requirement that schools must immediately notify the Department of a breach.
AUDIT FINDINGS

• Liberal arts colleges, public universities, and proprietary schools have had audit findings.

• 5-10% of institutions with audit findings didn’t know that GLBA is required for Title IV participation.

• Findings are occurring in all three areas
  • Some schools could not identify the point of contact.
  • Many did not have an incident plan in place.
  • Failure to perform a risk assessment is the most common audit finding.
EXAMPLES OF GLBA COMPLIANCE FINDINGS

• Use of accounts that are not password protected.

• Account passwords shared with staff members and student interns.

• Scanning and storage of PII to a network that can be easily accessed through any of the common administrator accounts.

• Discovered malicious programs, such as ones capable of capturing keystrokes typed on the keyboard (keylogger).
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.

- We will be asking for a corrective action plan.

- The Cybersecurity Team may provide assistance to the school to help address any findings.

LAST RESORT - If the Cybersecurity Team determines the institution poses a substantial security threat, FSA may implement an escalation process to ensure school accountability for protection of information.
National Institute of Standards and Technology (NIST) SP 800-171 Rev. 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

- Describes how to securely share Controlled Unclassified Information (CUI)
  - When agencies share CUI with a non-executive branch entity, they should enter into a formal agreement (32 C.F.R. § 2002.16)
  - Federal Mandate – requires compliance with a set of technical and administrative controls.
- The Department is looking at how this may apply to Institutions of Higher Education (IHE). We encourage schools to review and understand the standards defined in NIST SP 800-171.
# SP 800-171 CONTROL FAMILIES

<table>
<thead>
<tr>
<th>Families</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Media Protection</td>
</tr>
<tr>
<td>Awareness and Training</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>Physical Protection</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>Security Assessment</td>
</tr>
<tr>
<td>Incident Response</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>Maintenance</td>
<td>System and Information Integrity</td>
</tr>
</tbody>
</table>
CYBERSECURITY HYGIENE
CYBER HYGIENE

LEVEL 5
ADVANCED/PROGRESSIVE
OPTIMIZED:
Process implementation is standardized and optimized across all organizational units

LEVEL 4
PROACTIVE
REVIEWED:
Activities are reviewed and measured for effectiveness and higher-level management informed

LEVEL 3
GOOD CYBER HYGIENE
MANAGED:
A plan is established, maintained and resourced to perform all activities

LEVEL 2
INTERMEDIATE CYBER HYGIENE
DOCUMENTED:
Policies and practices are established and documented

LEVEL 1
BASIC CYBER HYGIENE
PERFORMED:
Practices are performed; but processes not institutionalized
BEST PRACTICE EXAMPLES

Form a hierarchical cybersecurity policy

Employ a risk-based approach to security

Segregate your data

Back up your data

Use multi-factor authentication

Handle passwords securely

Keep an eye on privileged users

Be wary of phishing

Raise employee awareness

Monitor third-party access to your data

Use the principle of least privilege
DEPARTMENT COMMUNICATIONS

• Dear Colleague Letters: GEN 16-12 & GEN 15-18
• Electronic Announcement:
  • Enforcement of Cybersecurity Requirements under the Gramm-Leach-Bliley Act
• FSA Website: https://ifap.ed.gov/fsa-cybersecurity-compliance
• CISA Resources: https://www.cisa.gov/cybersecurity
• NIST: https://www.nist.gov/cyberframework
QUESTIONS AND ANSWERS

Dan Commons
Email: FSASchoolCyberSafety@ed.gov