

# Session #25

## Cybersecurity – The Challenges Facing FAA's

Dan Commons

U.S. Department of Education

2019 FSA Training Conference *for Financial Aid Professionals*

# Agenda



- The Problem
- The Landscape
- The BOOM
  - Partnership
    - What is a Breach?
      - FSA Breach Process
    - 2019 Breaches and Case Studies
  - Best Practice
- Compliance
- Reporting Process
- Resources

# From the Headlines

**FORBES:**  
Data Breaches  
Expose  
**4.1**  
**Billion**  
Records In First  
Six Months  
of 2019



DATA BREACHES

**2 Billion**  
Records Exposed  
In Massive Smart  
Home Device Breach

**23 Million**  
Accounts Compromised  
in CafePress Hack

**REPORT:**  
2.3 Billion  
11 Million  
Including Private Ones  
**Exposed Online**

Lenovo confirms  
36TB data leak  
security vulnerability

**CAPITAL ONE DATA BREACH**

- 140,000 Social Security numbers
- 1 million Canadian Social Insurance numbers
- 80,000 bank account numbers
- Undisclosed number of names, addresses, credit scores, credit limits, balances, and other information

**CNN BUSINESS**

**HACKER ARRESTED IN MASSIVE CAPITAL ONE DATA BREACH**

PODIUM ORDER TOMORROW: BENNET, GILLIBRAND, CASTRO, BOOKER, BIDEN, HARRIS, YANG, GARRARD, INSLEE, DE BLASIO

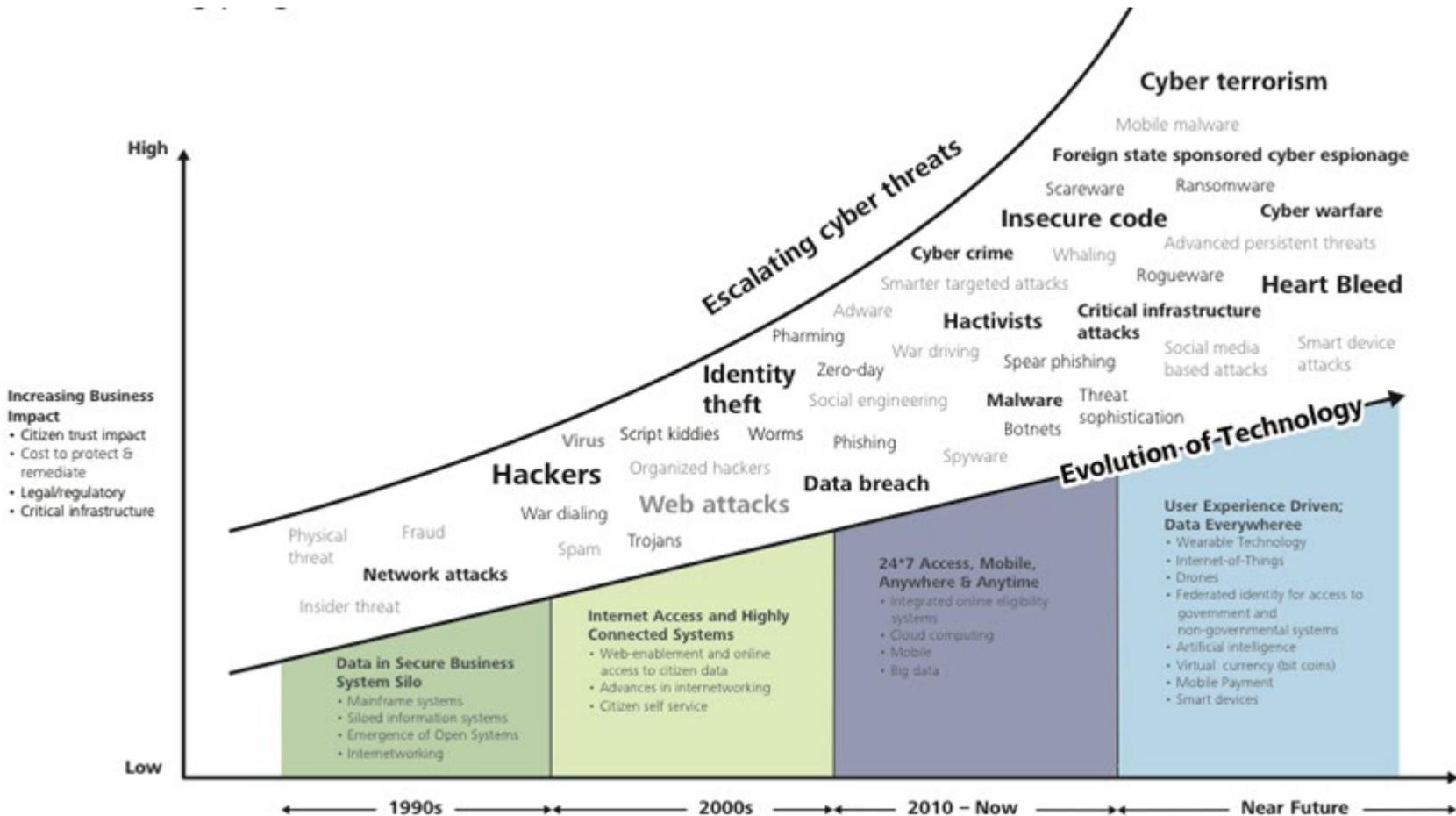
**CNN** NEW DAY

Data breaches  
increased  
**54%**  
in 2019 so far

# Breaches are a global problem



# Evolving Threat Landscape



# Threats Targeting Education Sector

## Threat Agents



Criminal Organization

Target student direct deposit information to redirect financial aid reimbursements to attacker bank accounts



Criminal Organization

Target student PII for resell on black market



Criminal Organization

Encrypting school systems for ransom



Nation-State Actors

Targeting university research and intellectual property

# Threats Targeting Education Sector

## Threat Trends



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



Sophisticated credential-theft attacks as a vehicle to compromise staff and student banking information



Compromise of unsecured cloud databases containing sensitive student information



# The BOOM

**Left : Proactive (\$\$)**

Technical  
Capabilities

Planning

Training

Staffing

OR



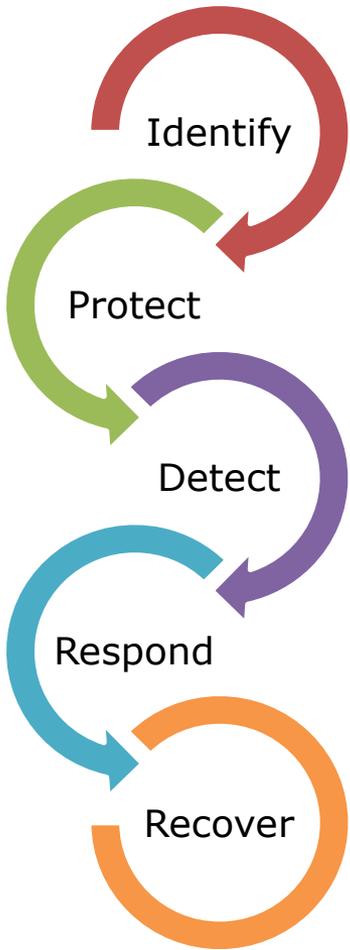
Technical  
Recovery

Financial  
Recovery

Reputation  
Recovery

**Right: Reactive (\$\$\$\$)**

# Education's Partnership with PSI's



**Identify**  
Cybersecurity Guidance

LEFT **Protect**  
Safeguard Guidance

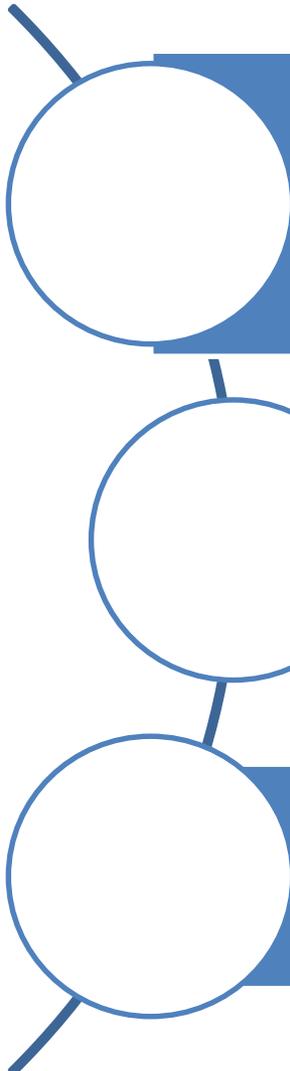


**Detect**  
Incident Report, Intake, & Investigation

**Respond**  
Containment Assistance, Root Cause Analysis, Site Visit, & Remediation

RIGHT **Recover**  
Fully system recovery and strengthening of security posture. Review of lessons learned and implementation of cyber practices.

# What is a breach?

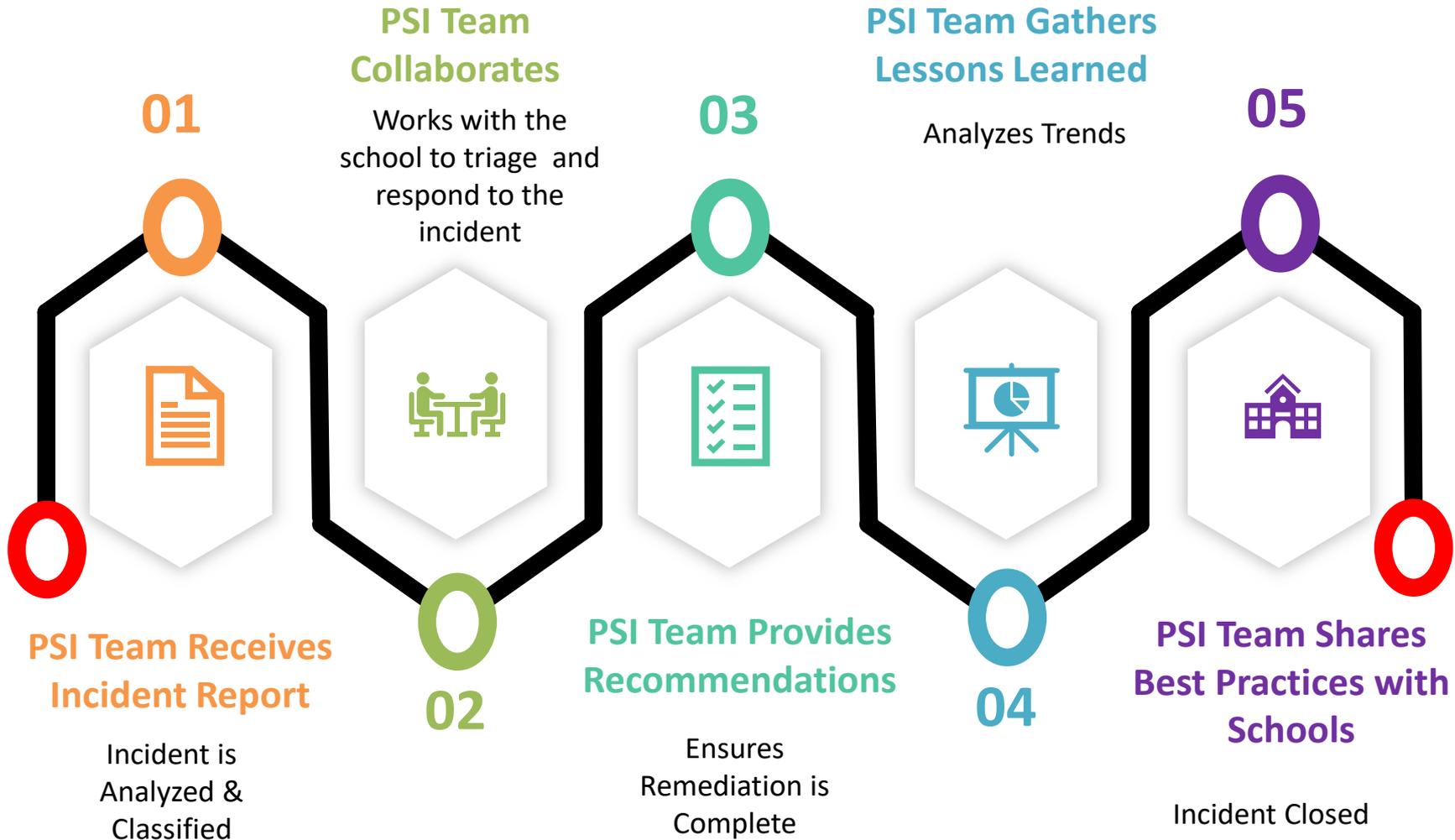


OMB M-17-12: “The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.”

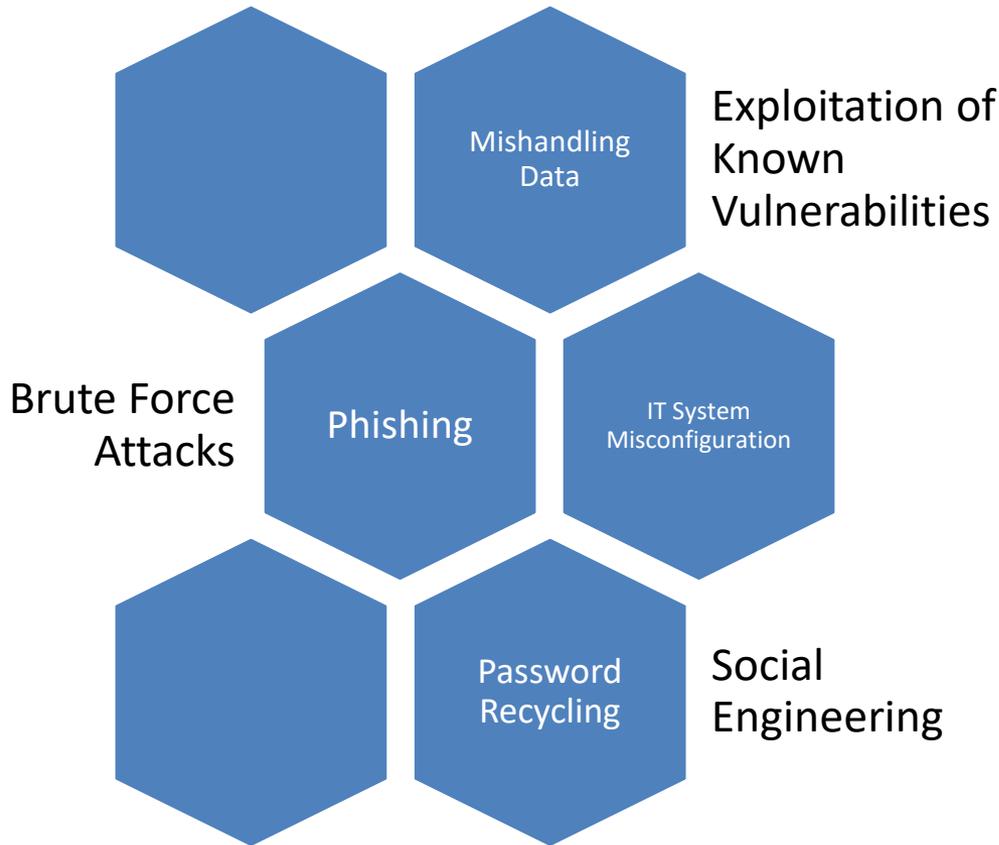
A “data breach” is “the unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.”

For Postsecondary Institutions, the data set is information obtained under or through the Title IV participation agreements.

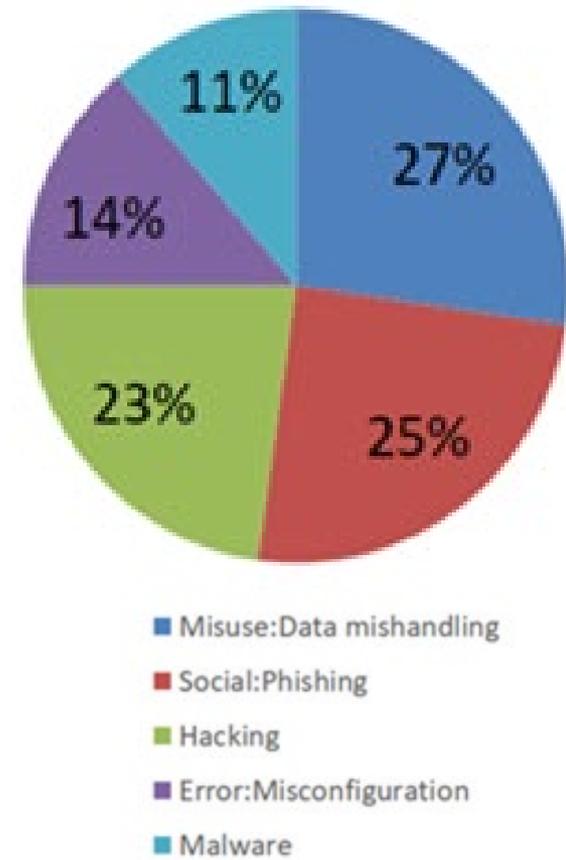
# FSA's PSI Breach Process



# Current Breach Causes



## 2019 PSI Breach Trends



# Ransomware

## Targeted Ransomware THE GROWING MENACE

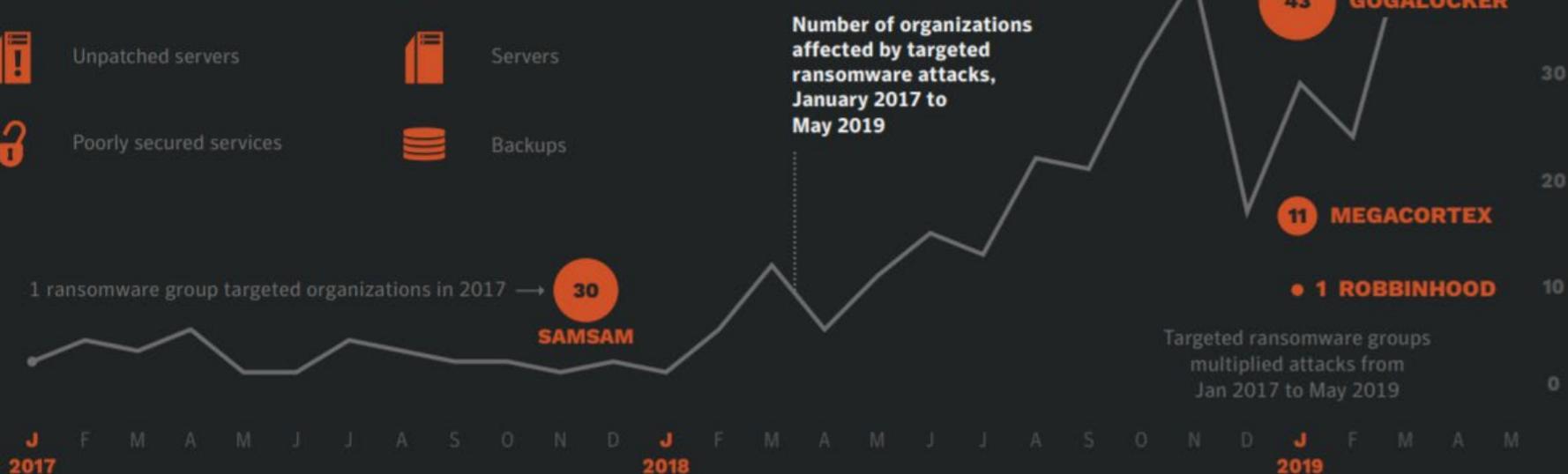
Greater the number of computers encrypted = greater the disruption caused = greater the chance victim will pay ransom

### Vectors

-  Spear phishing
-  Unpatched servers
-  Poorly secured services

### Under Threat

-  Computers
-  Servers
-  Backups



# 2019 Breach Trend

## EXAMPLE

### Phishing | Ransomware Attack

Phishing campaign that resulted in a Ryuk attack encrypted nearly all the IT infrastructure and disrupted the school's capability to function for days.

## How this could have been avoided...

- 01 Educate staff and conduct training on how to recognize phishing emails
- 02 Maintain backups offsite utilizing password protected mechanism that differs from regular authentication
- 03 Up-to-date firewalls can protect from inadvertent execution of virus-bearing attachments or malware
- 04 Install a robust antivirus program and update regularly
- 05 Install endpoint detection and response software to catch malware
- 06 Implement multi-factor authentication
- 07 Implement data loss prevention technologies

# 2019 Breach Trend

## EXAMPLE

### Data Mishandling

A faculty member inadvertently sent unencrypted email containing hundreds of student privacy records to the wrong recipient. Email was sent to an outside email address and could not be recalled.

## How this could have been avoided...

01

Implementation of a data loss prevention program that identified sensitive information before it is sent

02

Adopt robust policy that mandates that all sensitive information will be encrypted password protected

03

Ensure proper training for staff who are allowed access to sensitive or PII data

# 2019 Breach Trend

## EXAMPLE

### Account Compromise

A student's credentials were compromised and used to gain access to her email and financial aid portal resulting in direct deposit information being changed. Confirmation of account changes were sent to inbox but were deleted by an automated Outlook 'rule.'

## How this could have been avoided...

01

Implement a multi-factor authentication solution

02

Train and educate students on how to recognize phishing emails

03

Monitor log-in activity or utilize advanced email security to alert security staff to temporarily lock account

# 2019 Breach Case Study

## EXAMPLE

### Phishing Attempt

Financial aid administrator clicked on a phishing email and their password was captured. The attacker was then able to access the one drive account that contained unencrypted student data records for 2,000 students.

## How this could have been avoided...

01

Do not store student data in unapproved containers

02

Always encrypt student data

03

Educate staff on how to recognize phishing emails

04

Implement a multi-factor authentication solution

05

Implement a data loss prevention solution

# 2019 Breach Case Study

## EXAMPLE

### Laptop Theft

An instructor's laptop containing a spreadsheet was stolen. The spreadsheet had 1,000 student records (name, DOB, SSN, residency status, grades, classes taken, GPA, and financial award status). The laptop was not password-protected or encrypted. Three days later student PII was put up for sale on the dark web.

## How this could have been avoided...

01

Implement laptop and file encryption

02

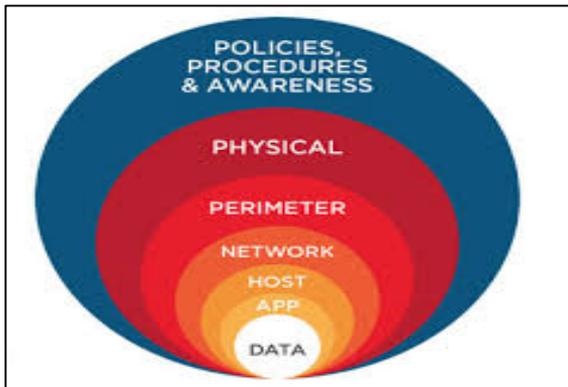
Limit types of PII faculty and staff have access to via a role-based approach

03

Implement a data loss prevention solution

# Best Practices for Data Protection

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



# Compliance Requirements

- FSA Program Participation Agreement (PPA) & Student Aid Internet Gateway (SAIG) Agreement
  - Title IV schools are responsible for protecting personal and financial information
  - Develop, implement, & maintain documented data security (info-sec) program and designate an employee(s) to coordinate the program
- Gramm-Leach-Bliley Act (GLBA, 2002)
- GEN 15-18 and GEN 16-12
- Family Educational Rights and Privacy Act (FERPA)
- Comply with your local state data breach reporting requirements

# How to Report a Breach to FSA

01

## SEND AN EMAIL

To...

[FSASchoolCyberSafety@ed.gov](mailto:FSASchoolCyberSafety@ed.gov); [cpssaig@ed.gov](mailto:cpssaig@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)

02

## 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)

03

The school shall report to FSA as they discover the breach so that FSA can work collaboratively with the PSI to resolve the incident

# Department of Education Resources

## Department of Education, Protecting Student Privacy Website

<https://studentprivacy.ed.gov/training/ferpa-101-colleges-universities>

- Free Web-based training
- Videos
- Webinars

# Federal Student Aid Resources

Cybersecurity Compliance page <https://ifap.ed.gov/eannouncements/Cyber.html>

Links to useful sites, documents, resources, regulations, POCs.

Cybersecurity Assessment Tool (CAT)

[https://ifap.ed.gov/eannouncements/attachments/FFIEC\\_CAT\\_form.pdf](https://ifap.ed.gov/eannouncements/attachments/FFIEC_CAT_form.pdf)

Automated self-assessment tool helps establish current risk profile and cybersecurity maturity

# NIST Resources

## NIST Special Publication 800-61:

Computer Security Incident Handling Guide provides guidelines on detecting and handling incidents

## NIST Special Publication 800-86:

Guide to Integrating Forensic Techniques into Incident Response

## NIST Special Publication 800-83:

Guide to Malware Incident Prevention and Handling for Desktops and Laptops

# Questions and Answers



Dan Commons

Email: [FSASchoolCyberSafety@ed.gov](mailto:FSASchoolCyberSafety@ed.gov)