BREAKOUT SESSION #19

How to Handle Data Mishandling

Margaret M. Glick

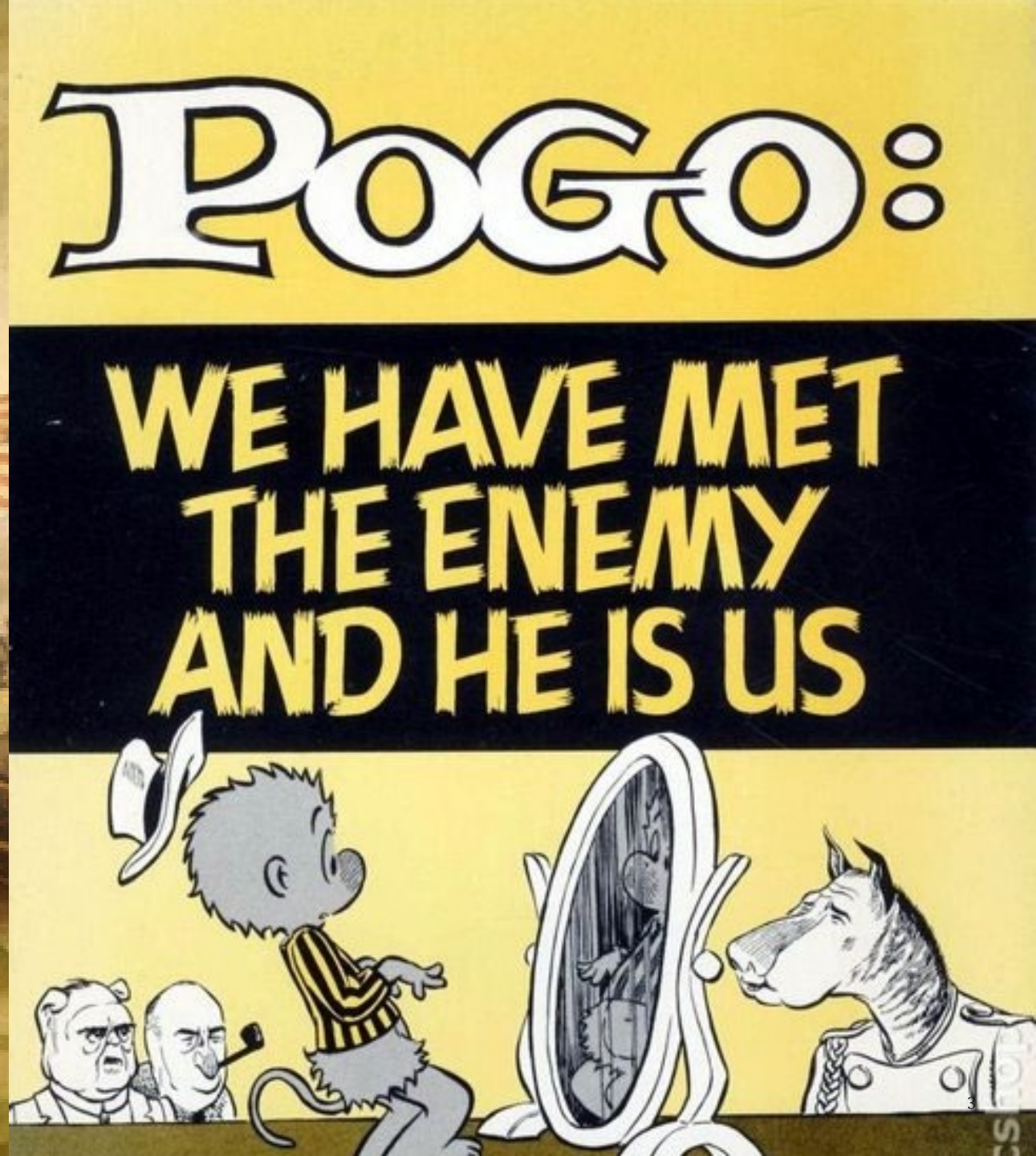
U.S. Department of Education

2023 FSA Training Conference for Financial Aid Professionals

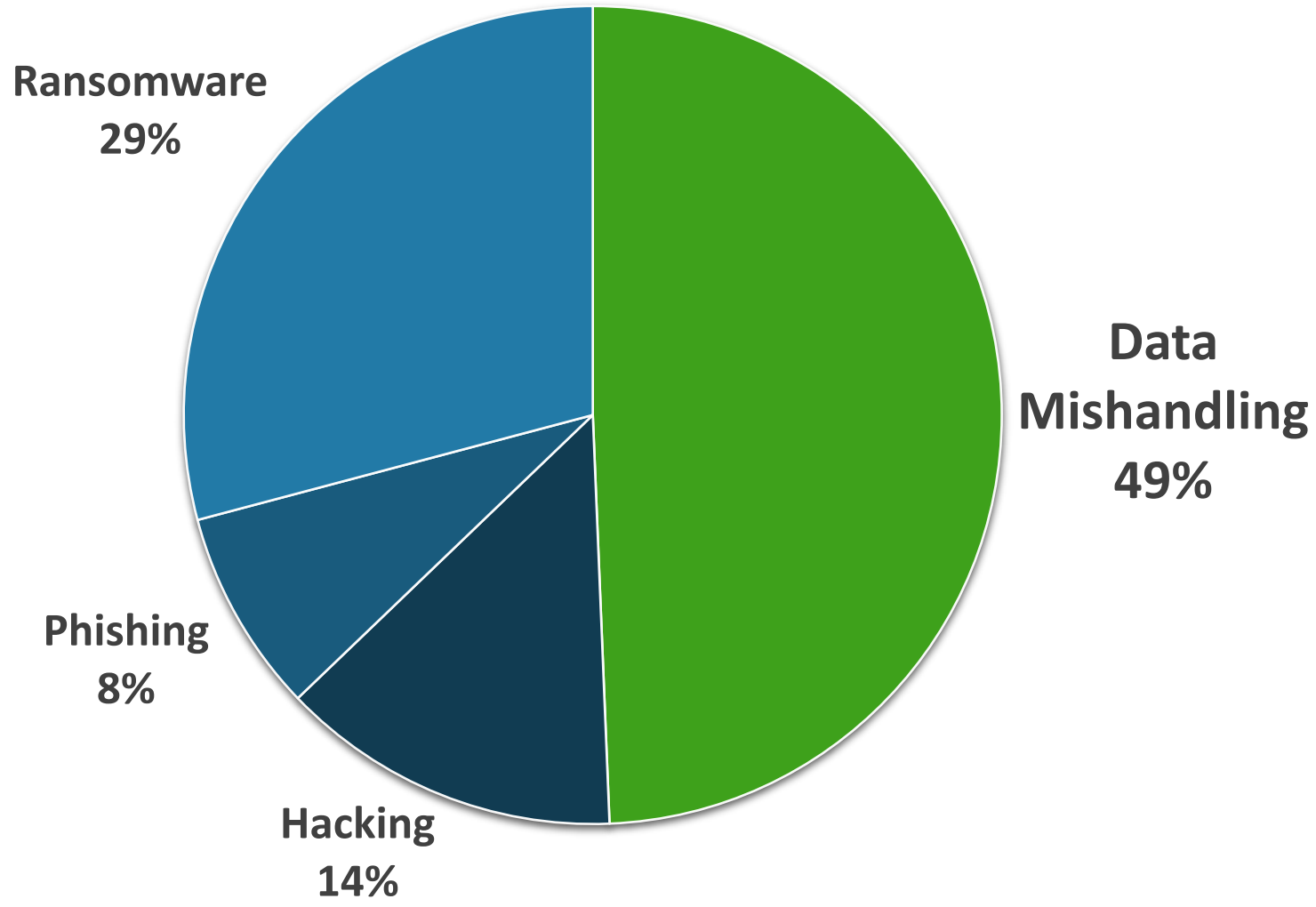
AGENDA

1. Understanding our role
2. How to: prevent data mishandling
3. How to: handle data disposal
4. How to: respond to data breach
5. About FSA and IHE Cybersecurity

"We have met the enemy and they are ours."
Commandant Oliver Hazard Perry, September 10, 1813



TOP CAUSES OF INCIDENTS REPORTED TO FSA

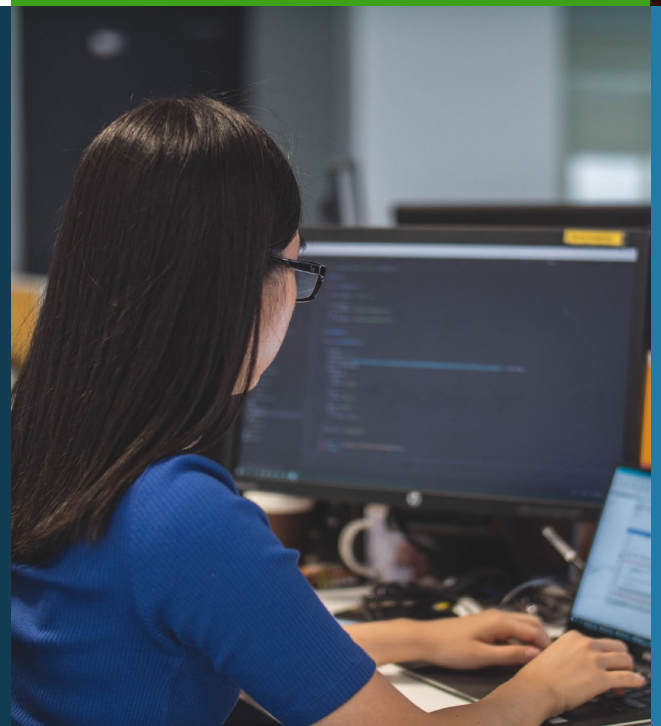


THE GOOD NEWS!

Good news: half of incidents we can prevent ourselves.

Emails containing sensitive student PII sent to wrong recipients

Sensitive information exposed during classroom presentations



Improper disposal of sensitive files

WHAT IS DATA MISHANDLING?

IHEs RECEIVE A LOT OF SENSITIVE DATA

CUI//SP-TAX

IRS

CUI//STUD

CUI//PRVCY

BETTER FAFSA®
BETTER FUTURE

ISIR

SOCIAL SECURITY
USA
ADMINISTRATION

FTI

12345678 1234 123 1234 5

DATA MISHANDLING

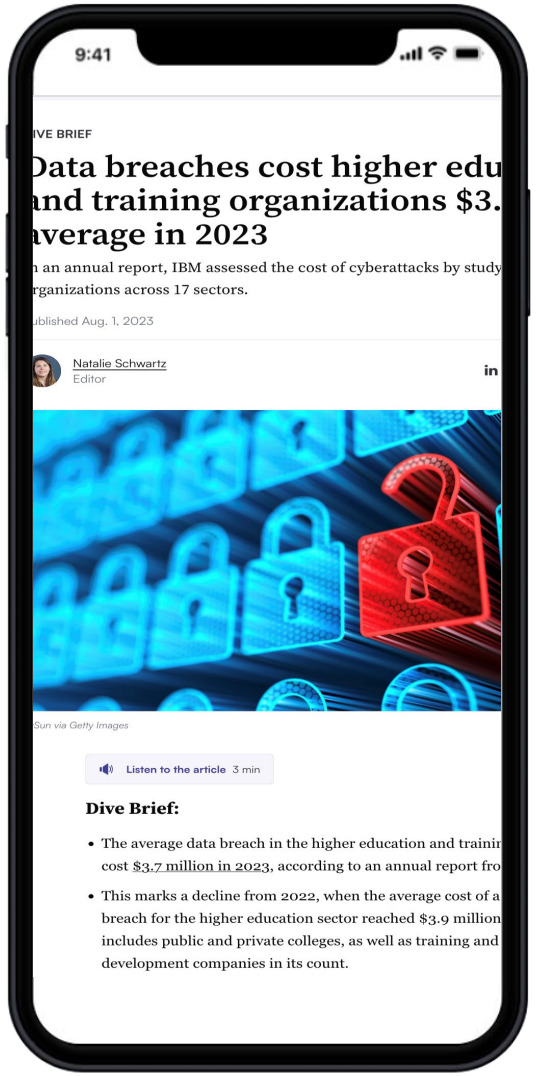
Data mishandling is the intentional or unintentional distribution of information to those who are not authorized to view, receive or use it.

Most often, data mishandling happens due to an employee mistake or carelessness, and the outcome of that error can vary in severity.

CONSEQUENCES

74% of all data breaches were the result of a human element

- Unauthorized disclosure of sensitive information
- Significant cost to remediate
- Loss of confidence in institution
- Lose access to critical systems



HOW TO PREVENT DATA MISHANDLING

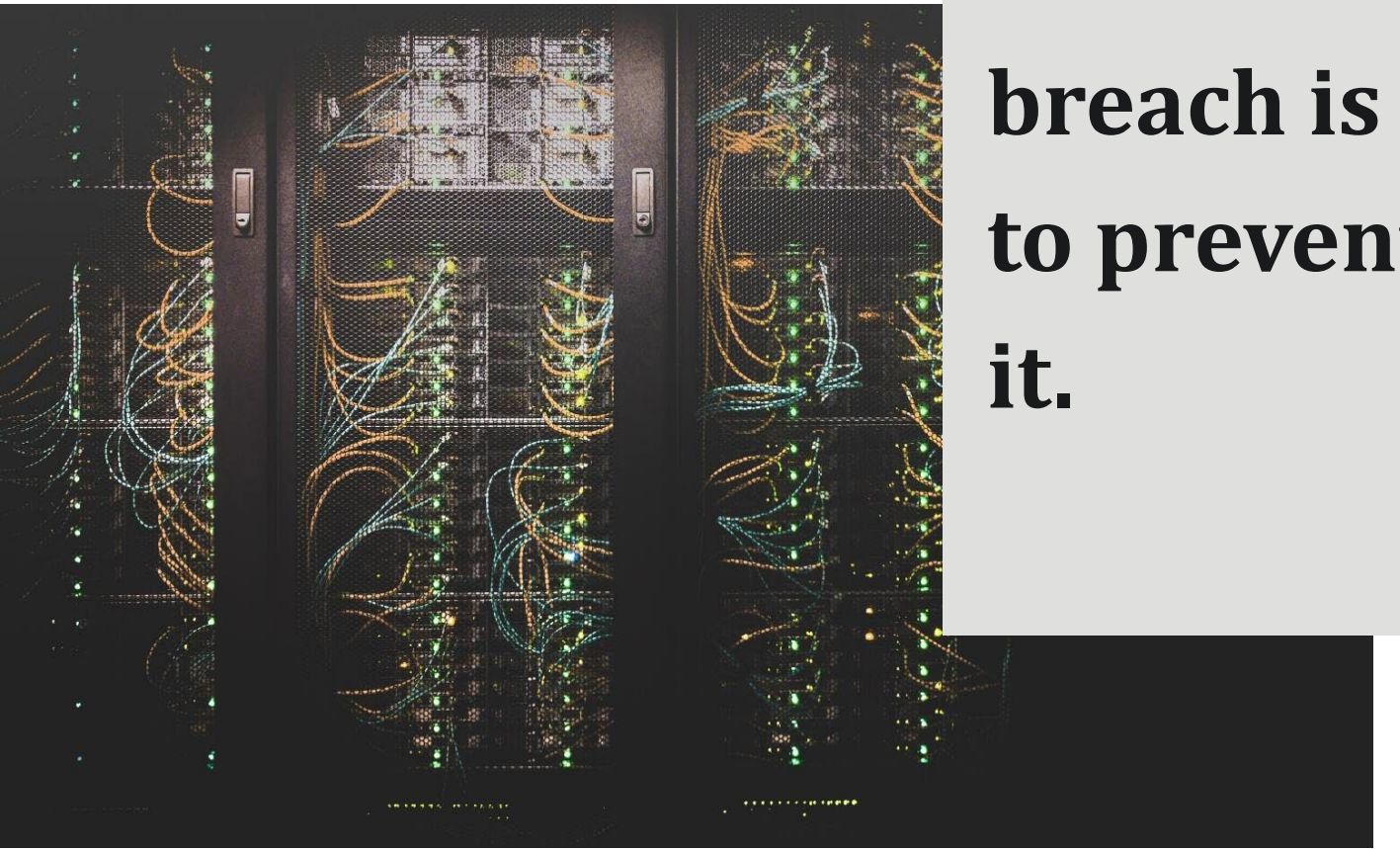
REDUCE DATA MISHANDLING

- Establish robust data access, storage, and handling policies and procedures
- Add checks and balances, like you already do for financial matters
- Hold department-wide training to raise awareness of data mishandling
- Make sure employees understand their roles and obligations, especially in the event of an incident
- Implement a Data Loss Protection system
- Enable email rules that flag content moving outside your organization

SEPARATION OF DUTIES

Good news, Data Mishandling is completely within our control. Fireman never go in a building without a buddy. Separation of duties. One person does, the other checks.

DATA MANAGEMENT BEST PRACTICES



The best way to avoid a breach is to prevent it.

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

- Make sure staff are fully aware of process and procedures when handling hard copies of data
- Slow down!
- Flag content moving outside and organization

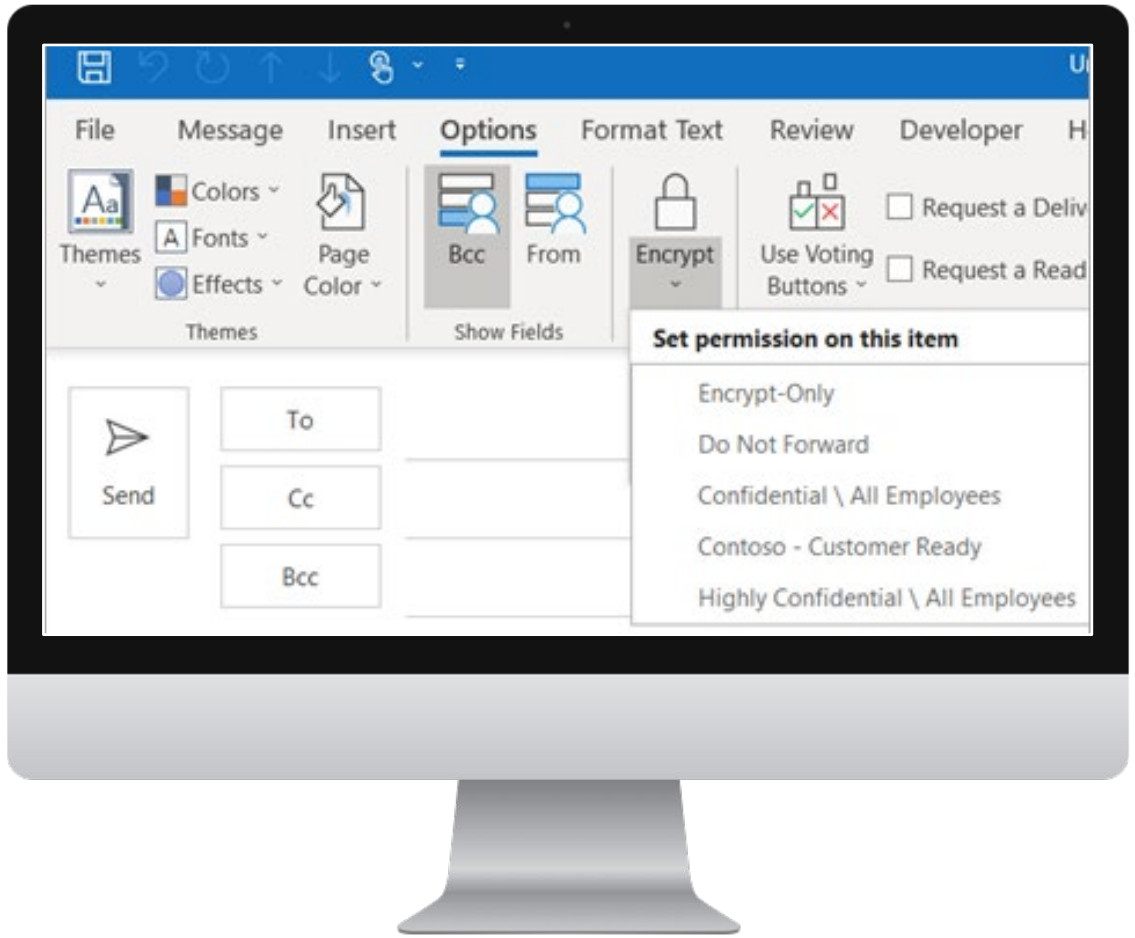
CHECKLISTS

Checklists came from the aviation industry. They cut air crashes significantly. Repeatable, standard procedures reduce mistakes and become second nature.

THE BEST WAY TO AVOID A BREACH

is to prevent it

- Encrypt emails
- When sending email always check to "To" box to make sure autofill did not select the wrong recipients
- Make sure contact lists and email address books are up to date
- Talk to your IT department about options for a Data Loss Protection system
- Double check listservs sent to third party processors
- Make sure staff know processes and procedures when handling hard copies of data



HOW TO HANDLE DATA DISPOSAL

WHAT IS MEDIA SANITIZATION?

Media sanitization is a process by which data is irreversibly removed from media, or the media is permanently destroyed.

Common media include physical documents, desktop and laptop computers, mobile devices, external hard drives, USB drives, and memory devices.

WHY PROPER DISPOSAL IS IMPORTANT

Proper data management, especially data destruction, is critical in protecting sensitive information against unauthorized access

HOW TO HANDLE A DATA BREACH

DATA BREACH CHECKLIST

☑	Validate the data breach
☑	Assemble incident response team
☑	Determine the scope and composition of breach
☑	Notify the data owners
☑	Ensure breach evidence is appropriately handled and preserved
☑	Collect and review breach response documentation and compile lessons learned

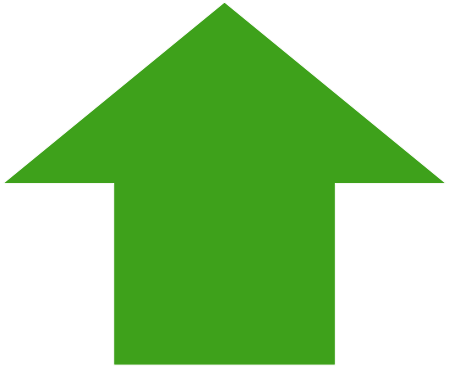
REPORT A BREACH

Schools are required by the SAIG and PPA Agreements to report all incidents of data mishandling immediately to FSASchoolCyberSafety@ed.gov

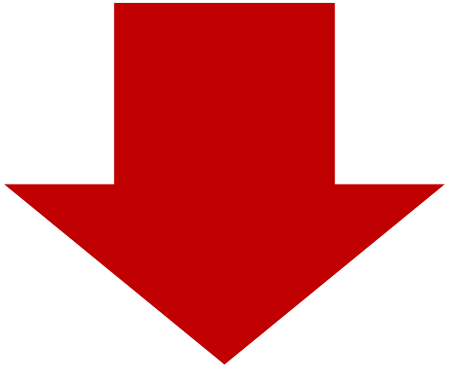
Or by using our Cybersecurity Intake Form.

Federal
Student
Aid

IHE CYBERSECURITY: OUR MISSION



Increase
Cybersecurity &
Privacy at IHEs



Decrease Risk
to FSA Data,
IHEs & Students

IHE Division Aligns -> with FSA's Enterprise Technology Directorate Priorities of Cybersecurity & SABER

FSA Strategic Objective 5.4, Improve cybersecurity detection, prevention, and protection ensuring data confidentiality, integrity, and availability

IHE PROVIDES TECHNICAL ASSISTANCE TO IHEs

- Incident Response
- Gramm-Leach-Bliley Act (GLBA) Audit Remediation
- Cyber Threat Information
- Outreach

INCIDENT RESPONSE

In **FY22**, we helped

300+

schools

Report a breach!

Report a breach with the Cybersecurity Intake Form.

Cybersecurity Breach Intake

Please complete the Cybersecurity Breach Intake Form.

Cybersecurity Breach Intake Form

All fields marked with an asterisk (*) are required.

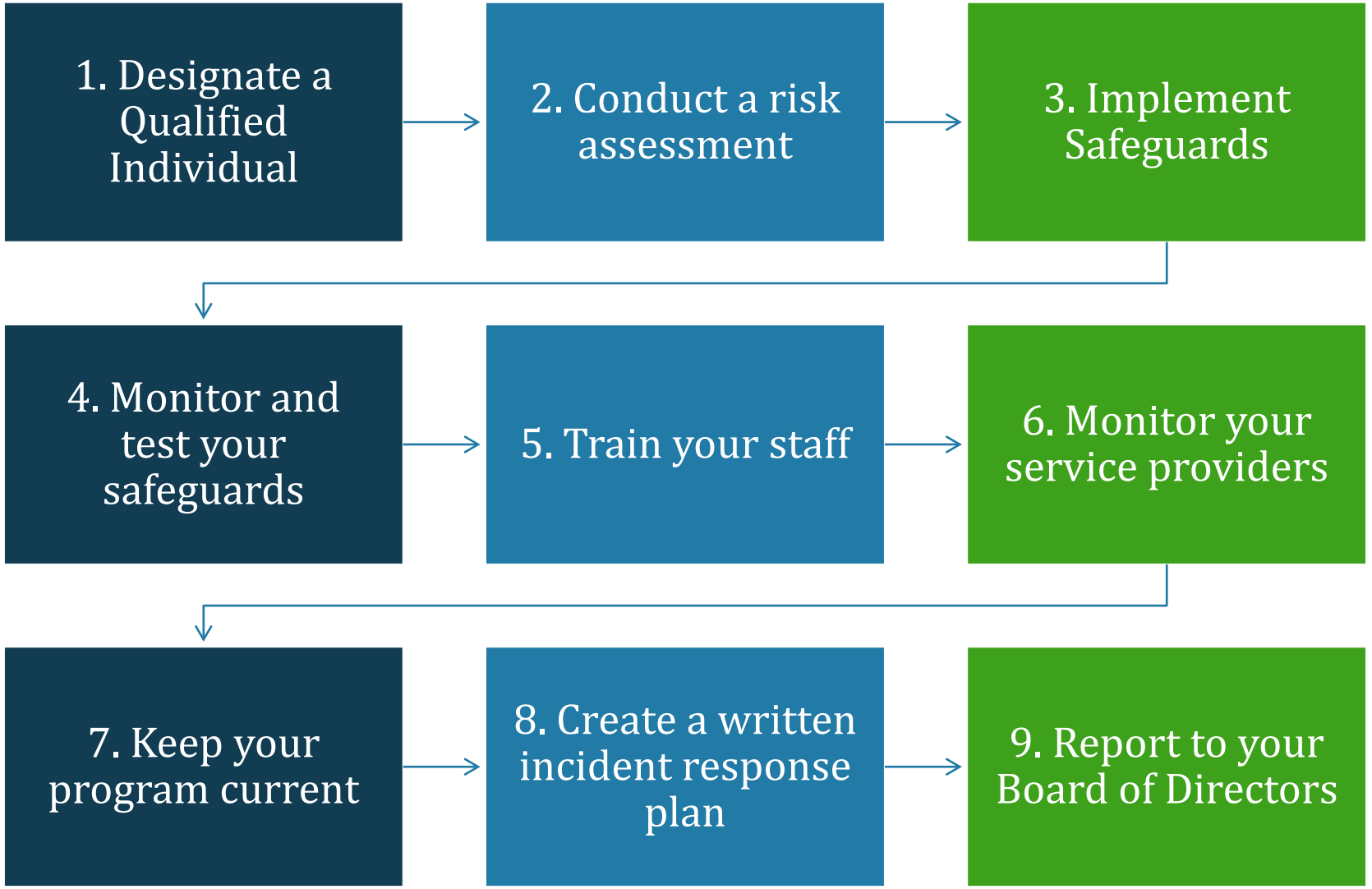
* **Date of Breach**
Suspected or Known

MM/DD/YYYY

* **Impact of Breach**
Number and type of records, etc.

* **Method of Breach**
Hack, accidental disclosure, etc.

GLBA ELEMENTS

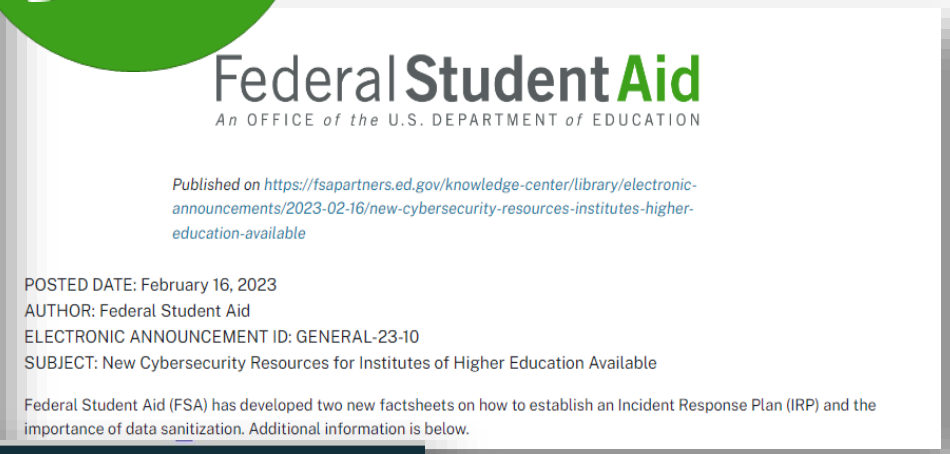


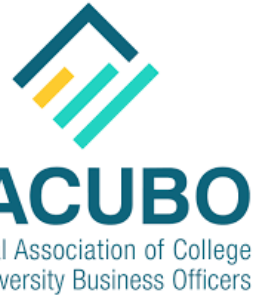
THREAT INFORMATION & OUTREACH

We proactively help schools through FSA's Cyber Threat Team, Federal threat information and dozens of Outreach events

OUTREACH

We created **19** events and communications in **FY22**





NATIONAL
CYBERSECURITY
ALLIANCE

IDENTITY DEFINED
SECURITY ALLIANCE

CHAMPIONS OF CYBERSECURITY

Virtual FSA Training Conference Nov 28-Dec 1 2023

FSA'S IHE CYBERSECURITY NEWSLETTER

- Actionable information, tips, and resources
- Sent quarterly to 20,000+ IT and compliance pros at IHEs

❑ To sign up, email FSASchoolCyberSafety@ed.gov with the subject line "Send me the FSA Cybersecurity Newsletter for IHEs"

QUESTIONS?

FSASchoolCyberSafety@ed.gov

FSA IS HERE TO HELP

BE PROACTIVE

REPORT BREACHES IMMEDIATELY

FSA CYBERSECURITY WEBSITE
HTTPS://FSAPARTNERS.ED.GOV/TITLE-IV-PROGRAM-ELIGIBILITY/CYBERSECURITY

CISA RESOURCES
HTTPS://WWW.CISA.GOV/CYBERSECURITY

NIST CYBERSECURITY FRAMEWORK
HTTPS://WWW.NIST.GOV/CYBERFRAMEWORK

APPENDIX

MEDIA SANITIZATION BEST PRACTICES

1. Create and abide by your school's media sanitization policy

2. Media sanitization method should be based on the sensitivity of the data, not the media type.

3. Data storage devices should be destroyed prior to disposal

MEDIA SANITIZATION BEST PRACTICES

4

Avoid using file deletion, disk formatting, and one-way encryption to dispose of sensitive data

5

Shred physical documents so they are safe for disposal or recycling.

6

Sanitize faulty storage media before returning it to the manufacturer for service or replacement

MEDIA SANITIZATION BEST PRACTICES

7

Verify all data sanitization procedures to ensure data is irretrievable

8

Document all media sanitization with signature confirmation

9

Third parties must agree that personally identifiable information (PII) be destroyed when no longer needed