

BREAKOUT SESSION #3

Protecting Student Data

Dan Commons

U.S. Department of Education

2022 Virtual FSA Training Conference for Financial Aid Professionals

AGENDA

1. Why *our* data?
2. Your role in protecting data
3. Real-life breaches and response
4. Cybersecurity best practices

WHY US?



17.8 million
FAFSA applications
processed*



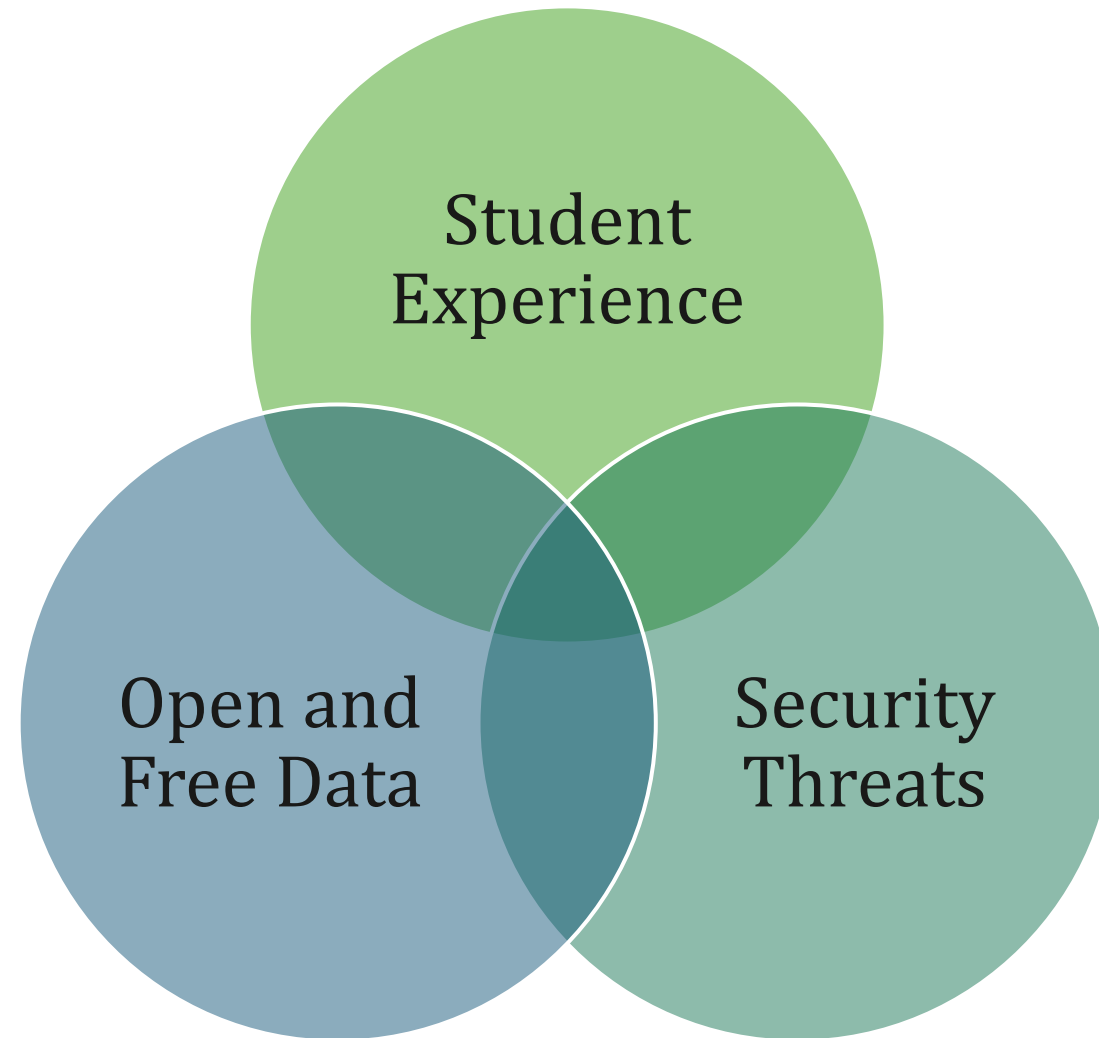
More than \$1.6
trillion in aid
awards



Billions of pieces of
personal, sensitive
information

FSA has an *enormous responsibility* to our applicants and taxpayers.

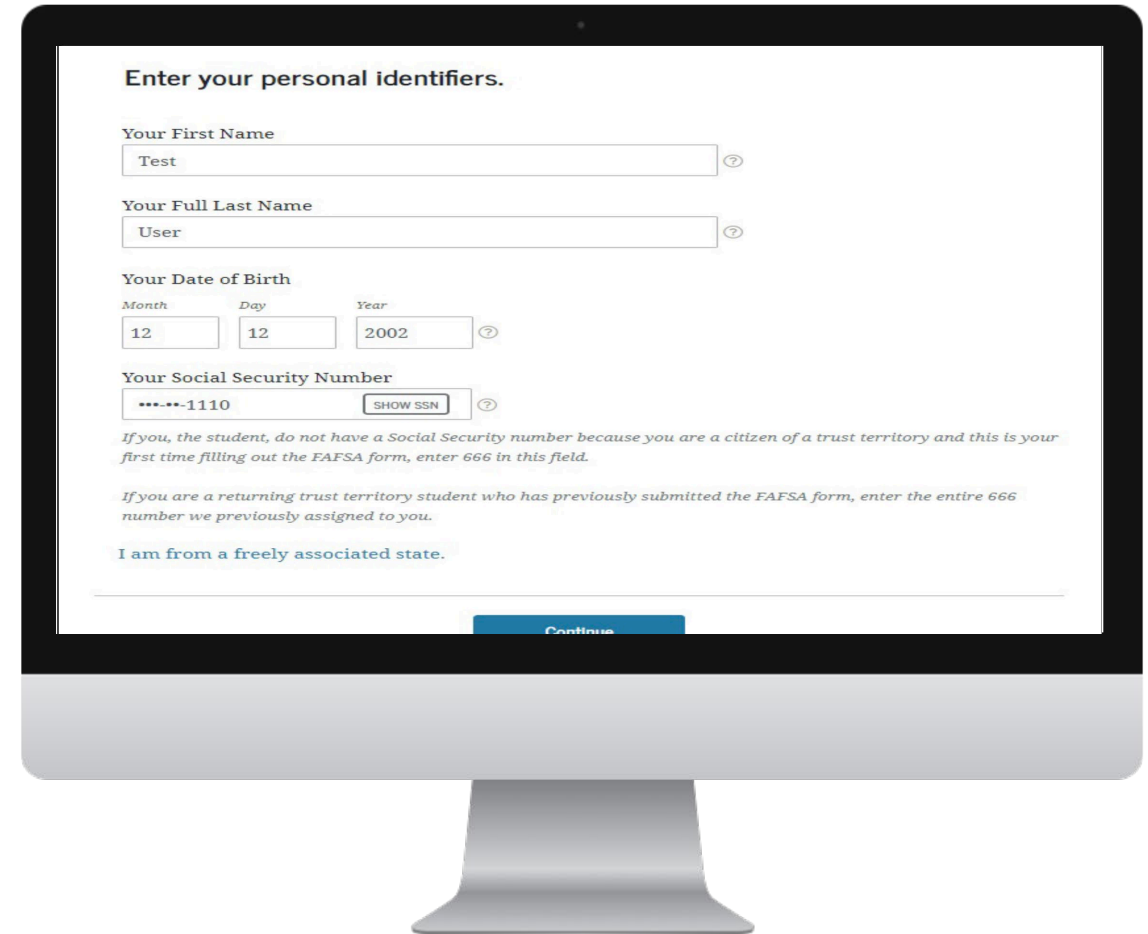
BALANCING ACT



WHY IS OUR DATA SO VALUABLE?

- FAFSA forms have:
- Social security numbers
- Financial information
- Federal and state tax returns

ALL OF THIS MEANS BIG \$\$ FOR HACKERS



The image shows a computer monitor displaying the FAFSA personal identifiers form. The form is titled "Enter your personal identifiers." and contains the following fields:

- Your First Name:** A text input field containing "Test".
- Your Full Last Name:** A text input field containing "User".
- Your Date of Birth:** Three separate input fields for Month (12), Day (12), and Year (2002).
- Your Social Security Number:** A text input field containing "•••••-1110" and a "SHOW SSN" button.

Below the form, there are two lines of instructional text:

- If you, the student, do not have a Social Security number because you are a citizen of a trust territory and this is your first time filling out the FAFSA form, enter 666 in this field.*
- If you are a returning trust territory student who has previously submitted the FAFSA form, enter the entire 666 number we previously assigned to you.*

At the bottom of the form, there is a checkbox labeled "I am from a freely associated state." and a blue "Continue" button.

FROM THE HEADLINES

Thousands of School Websites Went Down in a Cyberattack

'Golden Era' for Cyber Attacks as Criminals Take Advantage of Pandemic

Ransomware Feared in Weeklong Outage of Online Grading and Attendance Used by NYC School

Data Breach at University Impacts 30,000 Students

APT Targets Universities with Log4Shell Exploit Tools

Schools Remain Closed After Cyberattack



\$3.79 Million

THE AVERAGE COST OF A DATA BREACH IN THE EDUCATION SECTOR

- During the first quarter of 2021, the education sector accounted for nearly 10% of globally reported cyberattacks, compared with 7.5% during the first quarter of 2020.
- As of September 2021, 65 U.S. education data breaches reportedly affected approximately 555,000 records.



OUR SHARED RESPONSIBILITY

DEPARTMENT PRIORITY

Department and FSA Strategic Goals drive the focus.

TWO FOCUS AREAS:

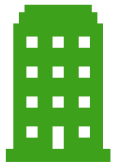
1. Improve student privacy data and cybersecurity controls of IHEs through outreach and communication to mitigate future cyber incidents and breaches.
2. Strengthen data protection and cybersecurity safeguards.



WHY COMPLY?



Regulatory law (Gramm-Leach-Bliley Act)



Industry group regulations



Professional obligation

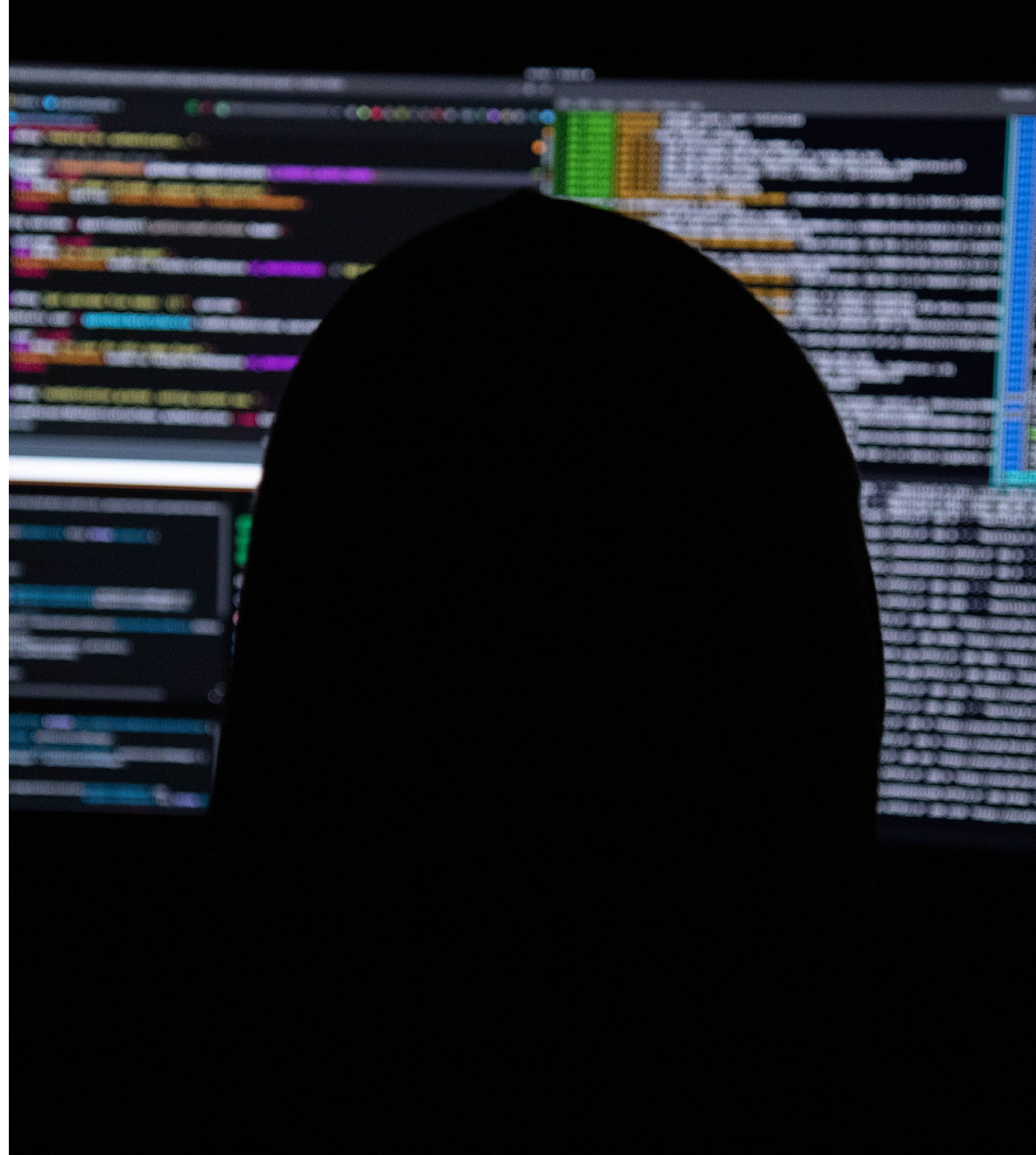
BE PROACTIVE!

- **Don't wait for someone else to tell you your cybersecurity measures need to be fixed.**
- Administrators who have adopted this mindset have been successful in their data protection objectives.



SECURITY CHALLENGES

- Lack of resources
- Small IT staffs
- Limited cybersecurity expertise
- Cost
- Awareness
- Fear



INSIDE A BREACH

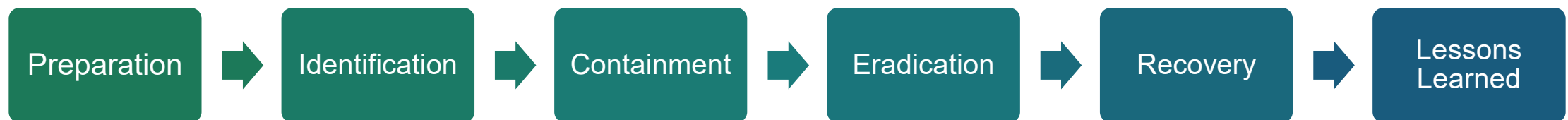
Actual breaches and how schools responded.



WHAT IS AN “INCIDENT”?

An incident is any negative event that takes place within an organization (malware attack, DoS attack, unauthorized access attempts).

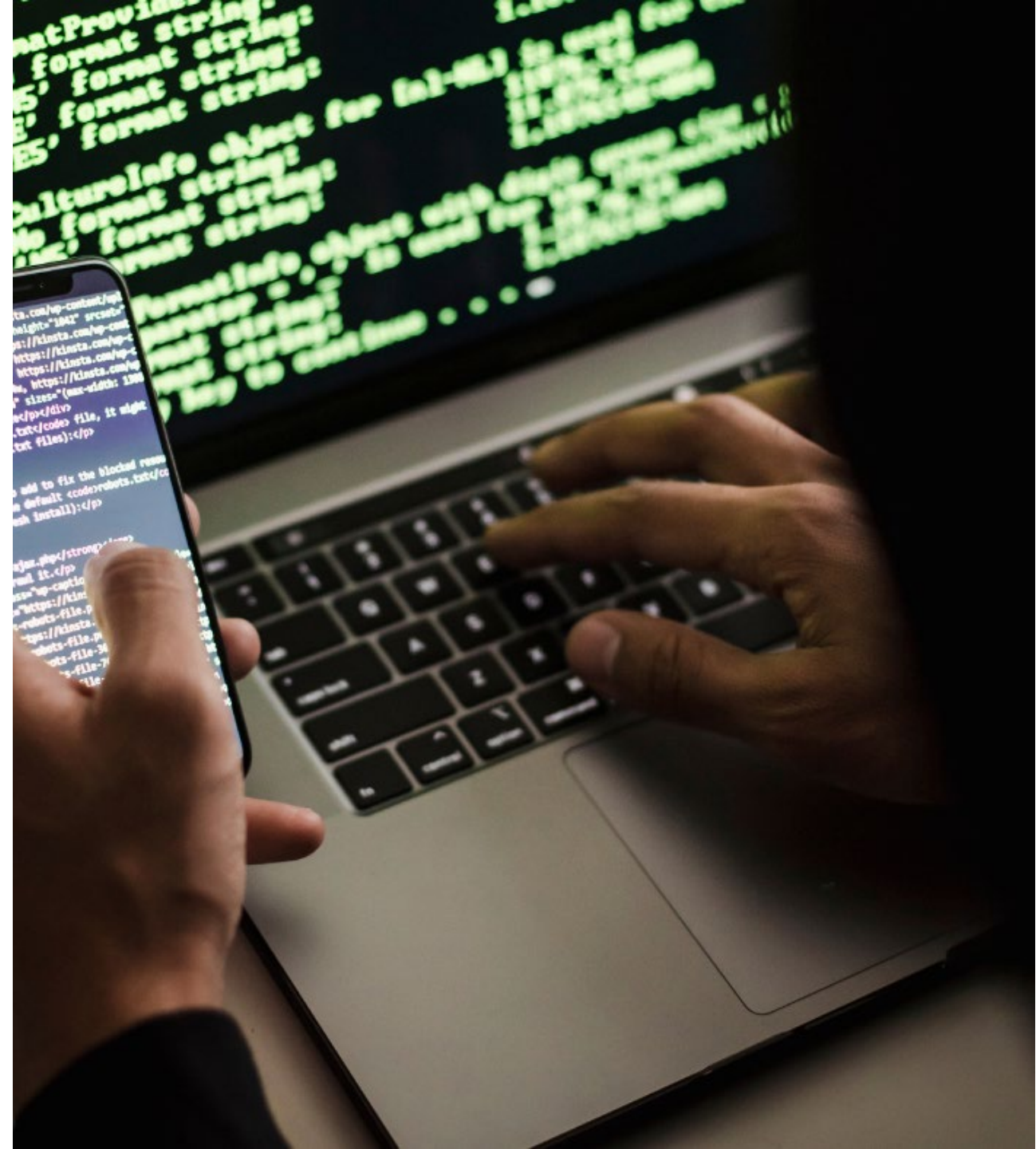
It's not a matter of if an incident will occur, but when, so every organization needs an **incident response plan**:



WHAT IS A “BREACH”?

One of most common incidents is a data breach. This occurs when confidential information has been exposed – either by accident or maliciously.

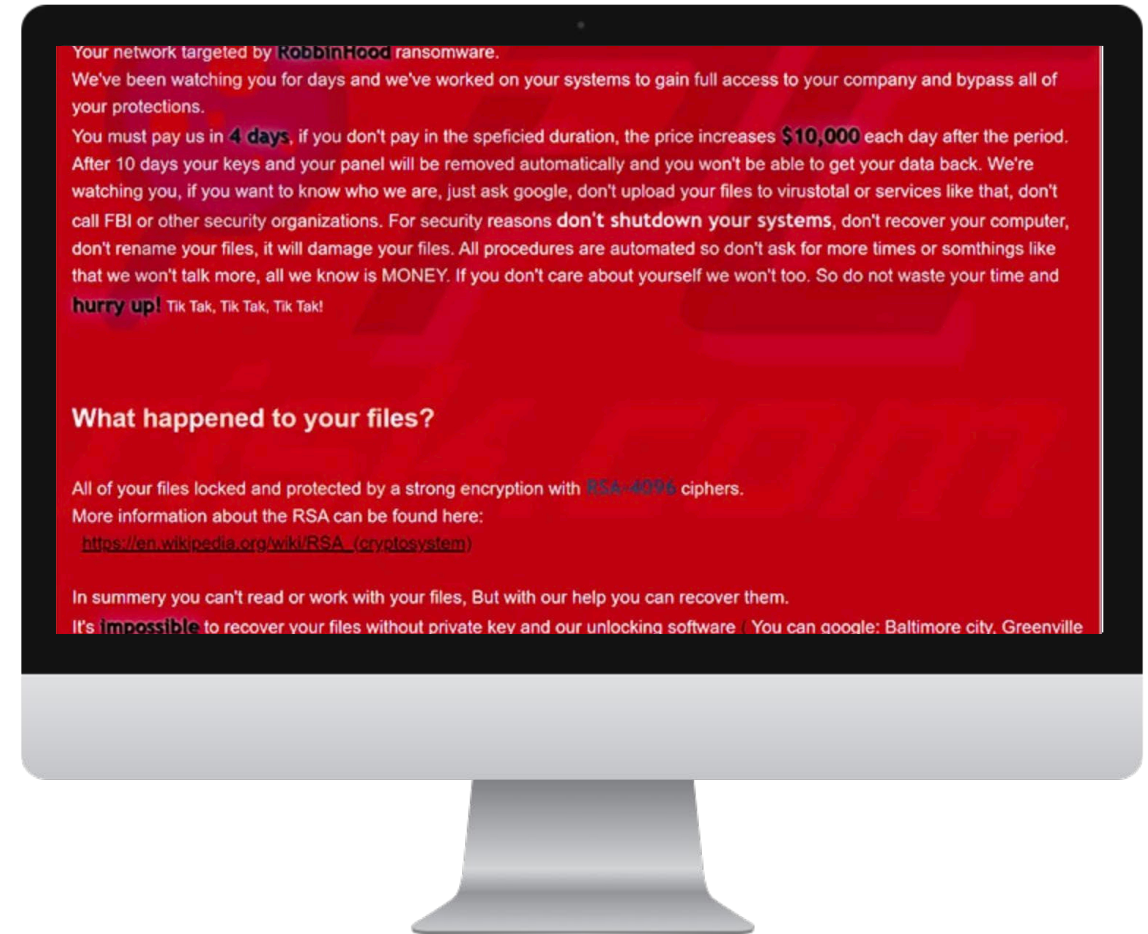
Data exfiltration is a type of data breach involving hackers or malware transferring data without authorization.



ROBINHOOD RANSOMWARE ATTACK

Victim: Medium-sized east coast university

- Phishing email launched trojan
- Monitoring system detected unusual activity
- Network was quickly shut down and online classes cancelled
- 6 laptops were encrypted, but no PII data was stored on those systems



RESPONSE CONSIDERED SUCCESSFUL

- Efficient detection, quick response
- Collaboration
- External and cloud data storage
- Existing policies



PYSA RANSOMWARE ATTACK

Victim: Small west coast college

- School negotiated with threat actor
- Threat actor claimed to have “deleted” the data
- IT department deleted all data in response
- No forensics trail



THIS INCIDENT LED TO...

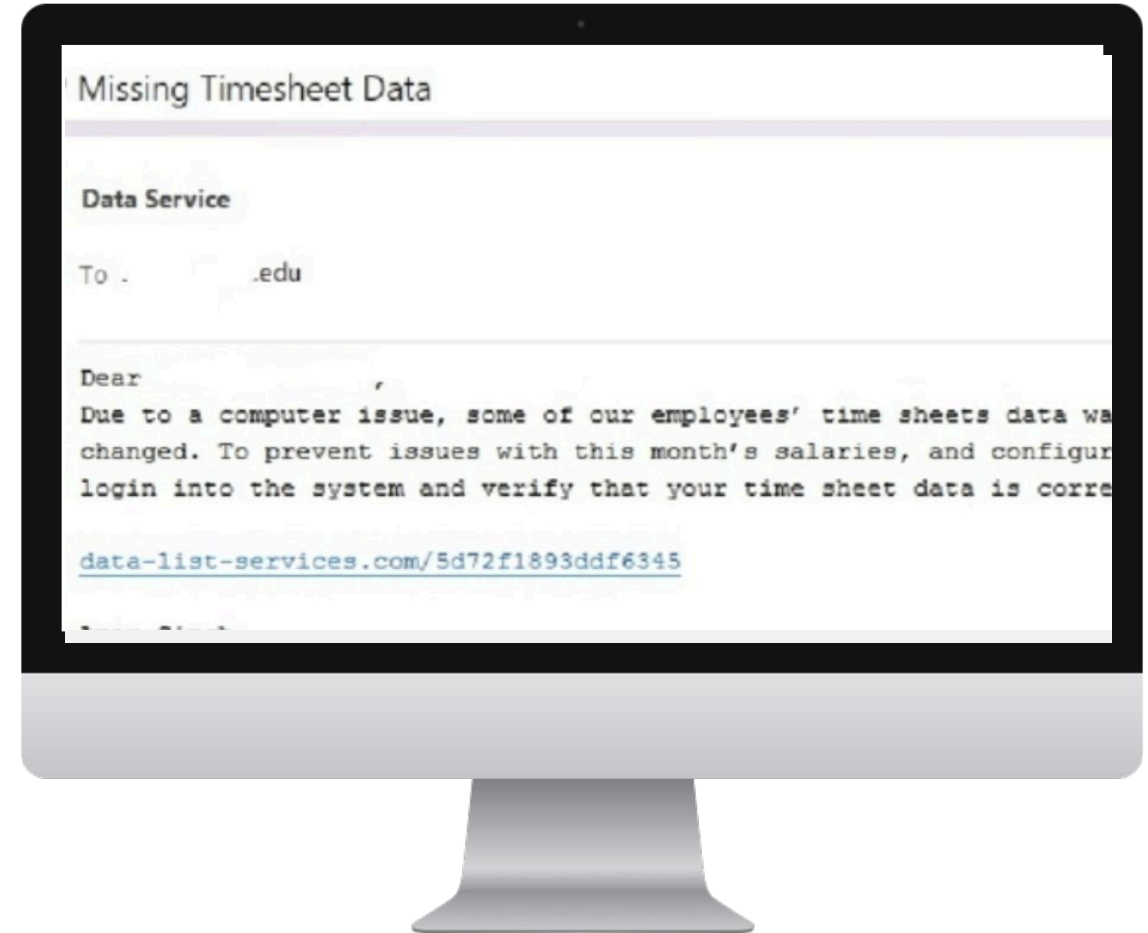
- ERP system, tens of thousands of accounts compromised
- School had to inform students of breach
- IT security risk assessment by independent IT auditor
- No remediation plans or safeguards found



PHISHING CAMPAIGN

Victim: Large southern university

- Considered “non-incident”
- IDPS systems
- Email security
- Network segmentation
- Vulnerability management
- Mature security posture and policies



KEY TAKEAWAYS



Have a plan



Assess threats regularly



Notify FSA immediately

IN THE EVENT OF A BREACH

CURRENT CYBERSECURITY BREACH INTAKE

Originally users would create an email with the information about a cybersecurity breach as seen on the previous Cybersecurity landing page below.

The screenshot shows a webpage titled "Cybersecurity" with the following content:

Cybersecurity

Federal Student Aid (FSA) recognizes the importance of strong data security. FSA collaborates with partners to protect personally identifiable information (PII), prevent data breaches, and provide robust methods to ensure proper cybersecurity is in place. Federal Student Aid has consolidated its cybersecurity compliance information and resources on this page. If you have any questions about the information included here, please contact FSASchoolCyberSafety@ed.gov.

Questions?

[FSA School Cyber Safety \(FSASchoolCyberSafety@ed.gov\)](mailto:FSASchoolCyberSafety@ed.gov)

FSA Cybersecurity Announcements and Guidance Page

You can access Technology Security Alerts, Electronic Announcements, Dear Colleague Letters, and other FSA Cybersecurity guidance on this Knowledge Center page.

Agreements and Regulations

Report a breach!

Email CPSSAIG@ed.gov.

Please include the following information:

- Date of breach (suspected or known)
- Impact of breach (# and type of records, etc.)
- Method of breach (hack, accidental disclosure, etc.)
- Information Security Program Point of Contact – Email and phone details
- Remediation Status (complete, in process – with detail)
- Next steps (as needed)


CYBERSECURITY BREACH INTAKE FORM

- A new Cybersecurity Breach intake form includes allows the user to enter the following information:
 - Date of Breach
 - Impact of Breach
 - Method of Breach
 - First Name
 - Last Name
 - Email Address
 - Phone Number
 - School/Organization Name
 - OPEID
 - Remediation Status
 - Provided details about remediation status
 - Next steps
- Once the form is submitted, an email is generated to Cybersecurity team with all the information from the form.

Cybersecurity Breach Intake Form

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

*** Date of Breach**
Suspected or Known

03/15/2022 

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

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

Information Security Program Point of Contact

* First Name	* Last Name
<input type="text"/>	<input type="text"/>
* Email Address	* Phone Number
<input type="text"/>	<input type="text"/>
School/Organization Name	OPEID
<input type="text"/>	<input type="text"/>

Information
The modernized NSLDS Professional Access website is coming soon. Re...

aining information here.

Title IV Participation Application

Maintain Eligibility

Audit Submission

Appeals

Cybersecurity

School Closures

FSA PARTNER CONNECT

Individuals involved in the administration of Title IV program eligibility and complete aid administration tasks. Explore policy and guidance in helpful tools, find training announcements, or link to other Federal Student Aid websites to manage Title IV program eligibility and complete aid administration tasks.

Log In

If you are a student or a parent, please visit [StudentAid.gov](#)

IFAP is now Knowledge Center

IHE CYBERSECURITY NEWSLETTER

- Actionable Information
- Sent Quarterly to 11,000 IT and Compliance Pros at IHEs
- To sign up and receive FSA's new cybersecurity newsletter, please email FSASchoolCyberSafety@ed.gov with the subject line: "Send me the FSA Cybersecurity Newsletter for IHEs."



FSA INCIDENT RESPONSE



FSA receives incident report



FSA team works with the school to triage and respond to the incident



FSA provides recommendations



FSA gathers lessons learned and analyzes trends



FSA shares best practices with schools

CYBER BEST PRACTICES

CYBER HYGIENE



5 ADVANCED

Cybersecurity processes are standardized and implemented across all departments

4 PROACTIVE

Practices reviewed and measured for effectiveness; high-level management informed

3 GOOD

A plan is established, maintained, and resourced to perform all security activities

2 INTERMEDIATE

Policies and practices are established and documented

1 BASIC

Practices are performed, but processes are not institutionalized

BEST PRACTICES

- Form a hierarchical cybersecurity policy
- Employ a risk-based approach to security
- Segregate your data
- Back up your data
- Use multifactor authentication
- Handle passwords securely
- Keep an eye on privileged users
- Raise employee awareness through training
- Monitor third-party access to your data
- Use the principle of least privilege
- Share this PowerPoint with leadership and information technology system departments

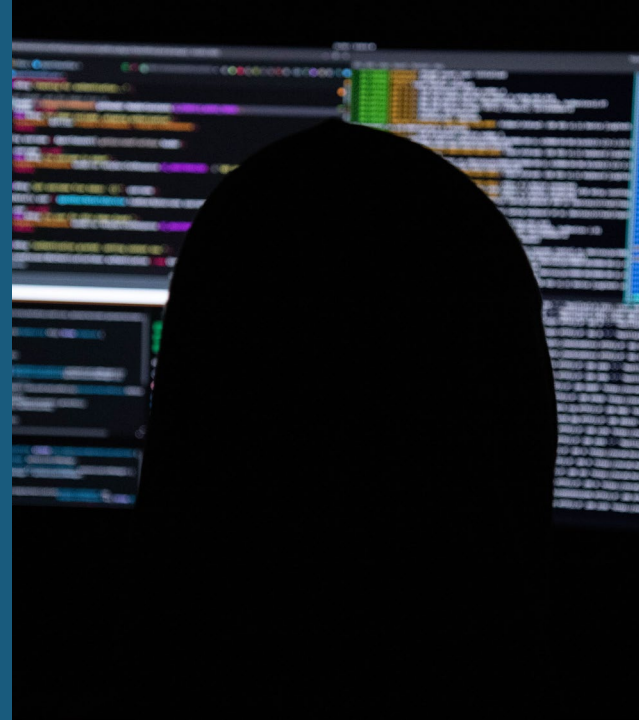


QUESTIONS?

FSA IS HERE TO
HELP



BE PROACTIVE



REPORT
BREACHES TO:

FSASchoolCyberSafety@ed.gov

RESOURCES

FSA CYBERSECURITY WEBSITE
[CYBERSECURITY | TITLE IV PROGRAM ELIGIBILITY \(ED.GOV\)](#)

CISA RESOURCES
[HTTPS://WWW.CISA.GOV/CYBERSECURITY](https://www.cisa.gov/cybersecurity)

NIST CYBERSECURITY FRAMEWORK
[HTTPS://WWW.NIST.GOV/CYBERFRAMEWORK](https://www.nist.gov/cyberframework)

RESOURCES (CONTINUED)

NATIONAL CYBERSECURITY ALLIANCE [HTTPS://STAYSAFEONLINE.ORG/RESOURCES](https://staysafeonline.org/resources)

NIST [SP 800-171 REV. 2, PROTECTING CUI IN NONFEDERAL SYSTEMS AND ORGANIZATIONS | CSRC \(NIST.GOV\)](#)

SELF-ASSESSMENT HANDBOOK FOR SP 800-171
[HTTPS://NVL PUBS.NIST.GOV/NISTPUBS/HB/2017/NIST.HB.162.PDF](https://nvlpubs.nist.gov/nistpubs/hb/2017/nist.hb.162.pdf)

CYBER SECURITY FRAMEWORK [HTTPS://WWW.NIST.GOV/CYBERFRAMEWORK](https://www.nist.gov/cyberframework)

CISA RESOURCES
[HTTPS://WWW.CISA.GOV/CYBERSECURITY](https://www.cisa.gov/cybersecurity) [STOP RANSOMWARE | CISA](#)

BLUEVOYANT
[CYBERSECURITY IN HIGHER EDUCATION REPORT BY BLUEVOYANT | BLUEVOYANT](#)

NOTES

The [Cybersecurity](#) landing page on Partner Connect is the resource where schools can find information to support their protection of federal data. FSA Cybersecurity Announcements and Guidance can be found on this [Knowledge Center](#) page.

Additional information about FERPA, Information Security, and Breach Reporting Requirements can be found in the [2021-2022 Federal Student Aid Handbook](#), Volume 2 - School Eligibility and Operations, Chapter 7: Record Keeping, Privacy, & Electronic Processes p.2-209 through 2-220. [PDF location](#) on Partner Connect.

All agreements to protecting data are reiterated in Program Participation Agreements (PPA) and Student Aid Internet Gateway (SAIG) Agreements.