BREAKOUT SESSION #2

Surviving a Cyber Attack: Does Your Institution Have What It Takes?

Margaret Glick
U.S. Department of Education
2022 Virtual FSA Training Conference for Financial Aid Professionals

AGENDA

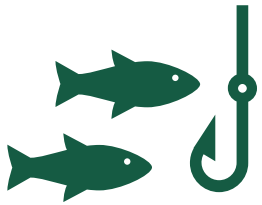
1. Introduction
2. Biggest Cybersecurity Challenges for Institutions
3. State of Ransomware in the Education Sector
4. Panel Discussion
5. Best Practices and Mitigation
6. Post-Incident Steps
7. Questions

BIGGEST CYBERSECURITY CHALLENGES

For Educational Institutions

Increased Frequency of Cyber Attacks

Limited IT Resources



Building Cyber Aware Culture

001001010101100011
001000100011110010
100100010010001010
01**530,000,000**10101
011100100010101001
010101101010110001
011**250,000,000**1010
010110101001011010
110101100101100011
0110**220,000,0000**10
110101001001010101
100011001101001010
100101101010010110

History has shown that even the most formidable fortresses can be occupied. In 2021:

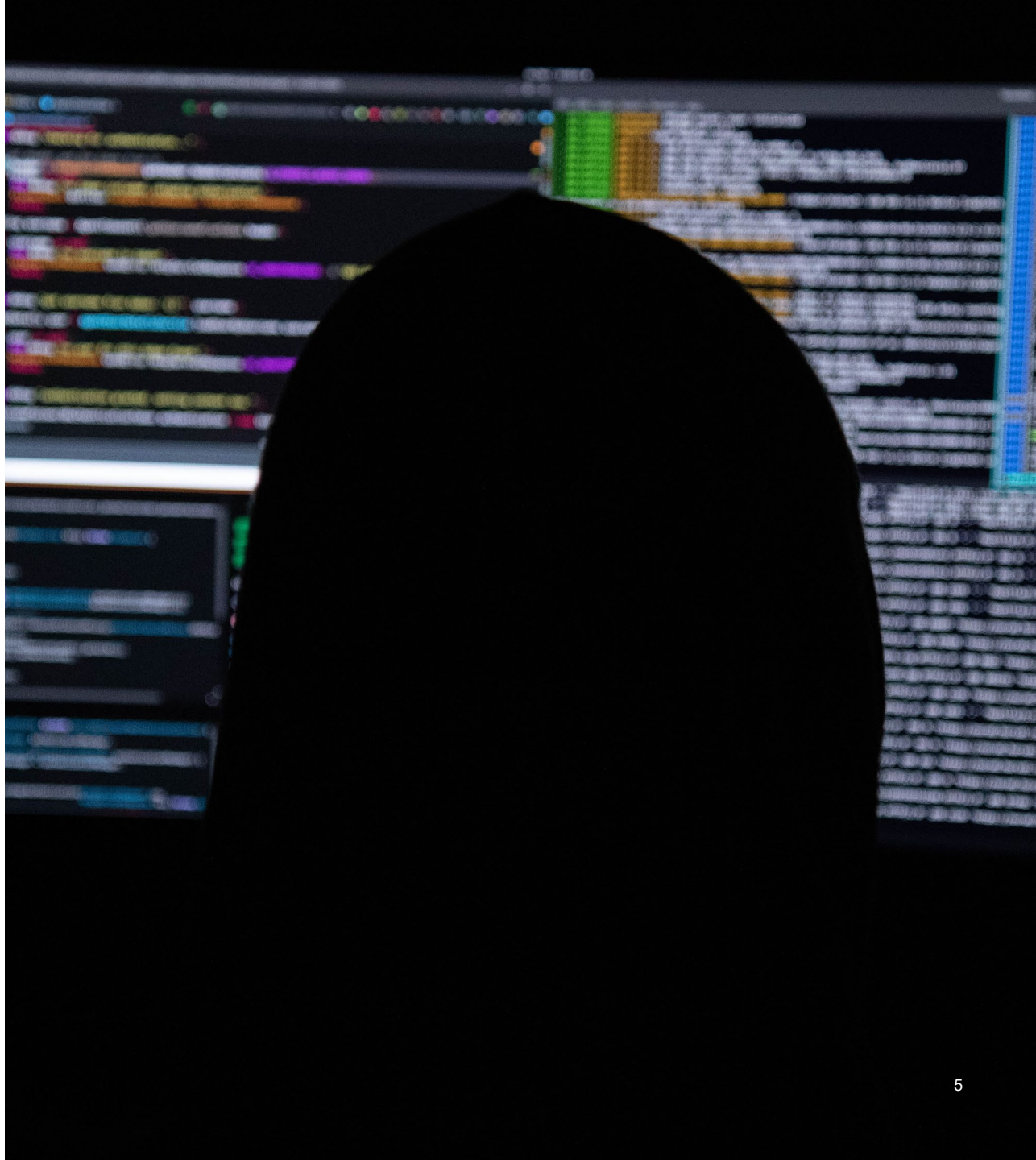
Facebook – 530 million users exposed

Microsoft – 250 million customer records exposed

Experian (Brazil) – 220 million records exposed, creating the largest personal data breach in Brazilian history

WHY ARE SCHOOLS FREQUENT TARGETS?

- Collect personal data, including financial information
- Have valuable research data and intellectual property
- Open environments
- FSA is assisting an average of 3 schools per day



STATE OF RANSOMEWARE IN EDUCATION

44% of educational institutions were hit by ransomware

58% said cybercriminals succeeded in encrypting their data

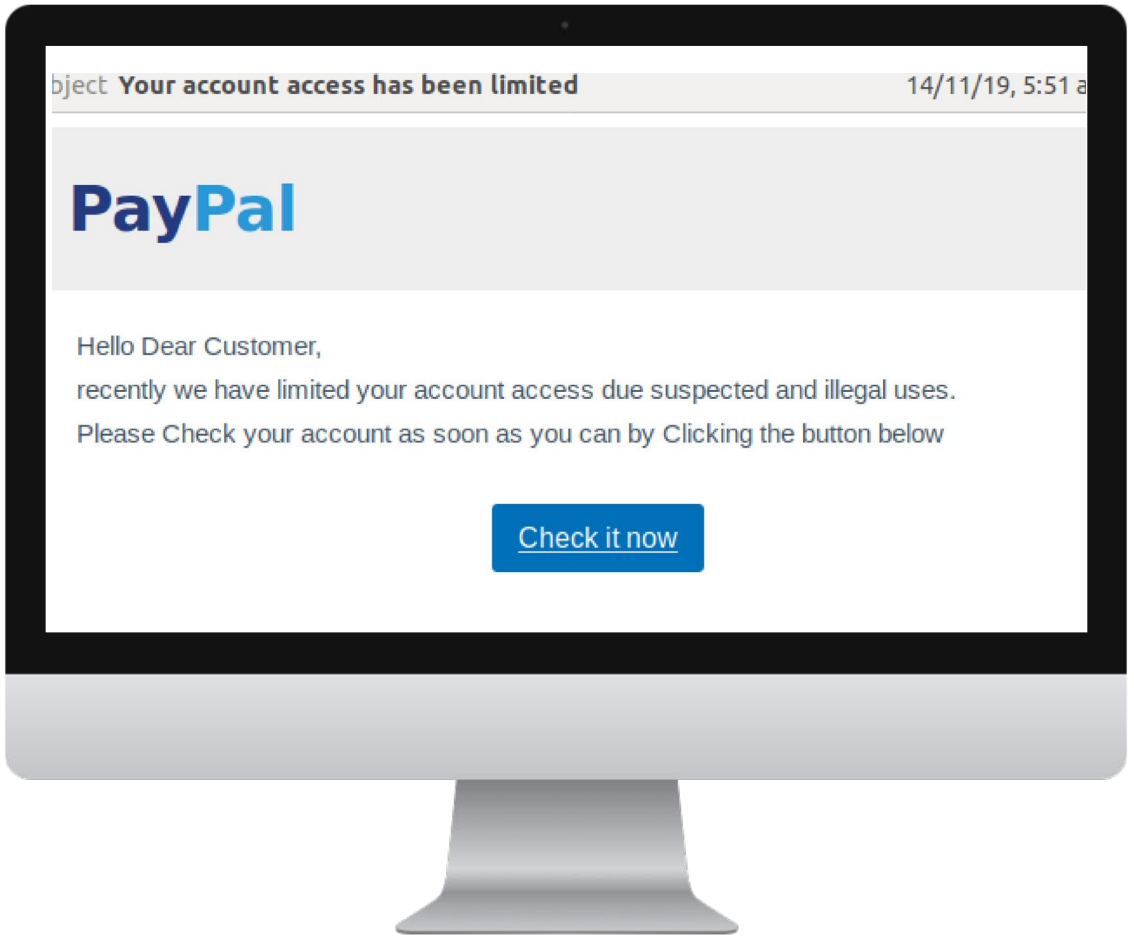
35% paid ransom to get encrypted data back

$112,000 average ransom payment

However, those who paid the ransom got back **only 68% of their data**

ENTRY POINTS

1. Phishing/Malicious links
2. Unpatched vulnerabilities
3. Weak access management
4. Unsecured remote access ports
5. Weak passwords protocols



BREACH CONSEQUENCES ARE DEVASTATING

Lost access to critical systems

Stolen data

Cost – $2.7 million average cost of data breach in 2021

Reputational damage

Permanent school closure

PANEL DISCUSSION WITH IHE CYBERSECURITY PROFESSIONALS

Trisha Clay, CIO, Hudson County Community College

Leo Howell, CISO, Georgia Tech

Tom Dugas, Assistant VP and CISO, Duquesne University

BEST PRACTICES FOR PREVENTION

- Implement multi-factor authentication
- Regularly patch vulnerabilities
- Conduct phishing training
- Regularly update hardware, software, and systems
- Manage third-party risk
- Establish offsite data storage
- Zero Trust Architecture (ZTA) framework

BEST PRACTICES FOR MITIGATION

- Build an Incident Response Plan
- Enforce MFA for all users
- Continuous network monitoring
- Centralized patch management
- Configure and secure internet-facing network devices

HOW TO MITIGATE AN ATTACK IN PROGRESS

1. Shut off networks and systems to limit spread.
2. Bring systems back online only after they are checked and cleared of infection.
3. Block IP addresses that were related to the attack.
4. Reset credentials for potentially affected accounts.

POST-INCIDENT STEPS

1. Perform forensic analysis on server, network, and application logs from recent weeks.
2. Restore data from backups.
3. Notify law enforcement of any criminal activity.
4. Report incidents immediately to cpssaig@ed.gov and FSASchoolCyberSafety@ed.gov and include:
   - ✓ Institution name
   - ✓ OPEID (school code)
   - ✓ Incident date (if known)
   - ✓ Incident discovery date
   - ✓ Technical details (if known)
   - ✓ Extent of impact
   - ✓ Remediation status
   - ✓ Institution point(s) of contact

RESOURCES

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

INCIDENT RESPONSE PLAN
HTTPS://NVLPUBS.NIST.GOV/NISTPUBS/SPECIALPUBLICATIONS/NIST.SP.800-61R2.pdf

CYBERSECURITY SELF-ASSESSMENT
HTTPS://NVLPUBS.NIST.GOV/NISTPUBS/HB/2017/NIST.HB.162.PDF

CYBERSECURITY FRAMEWORK FOR RISK MANAGEMENT
HTTPS://WWW.NIST.GOV/CYBERFRAMEWORK

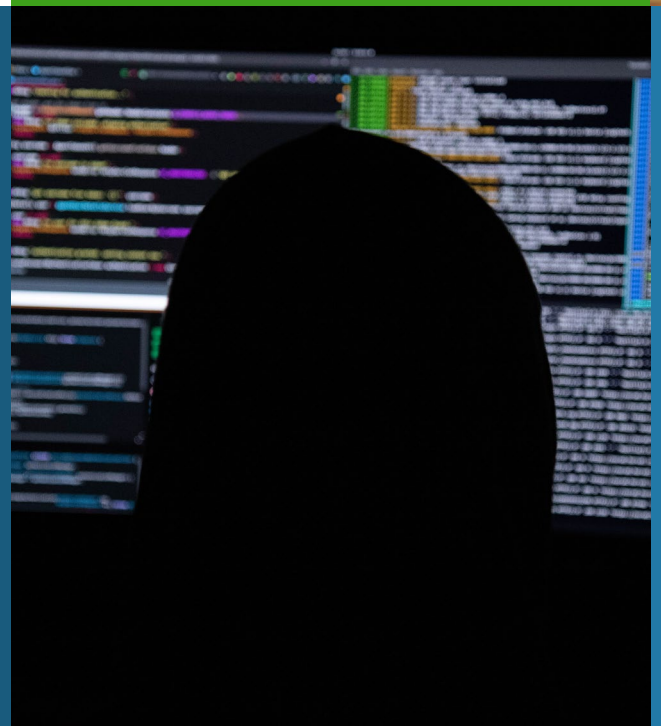
OTHER CYBERSECURITY RESOURCES FROM CISA
HTTPS://WWW.CISA.GOV/CYBERSECURITY
HTTPS://WWW.CISA.GOV/STOPRANSOMWARE

QUESTIONS?

FSASchoolCyberSafety@ed.gov

FSA IS HERE TO HELP

REPORT BREACHES IMMEDIATELY



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."