

Session #24

Protecting Sensitive Data and Minimizing Fraud Through an Integrated Approach

Ms. Kathy Zelnik, Mr. Wally Coy, and Ms. Stephanie Powell
U.S. Department of Education
2019 FSA Training Conference for Financial Aid Professionals

Agenda

1

Objectives

2

Introduction to Enterprise Risk Management and Institutional Leadership Context

3

Cyber Security Risk Management

4

Fraud Risk Management

Objectives



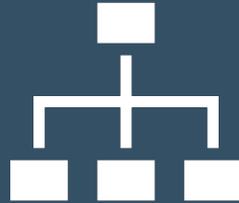
To introduce Enterprise Risk Management and the Increasing Complexity of Institutional Leadership



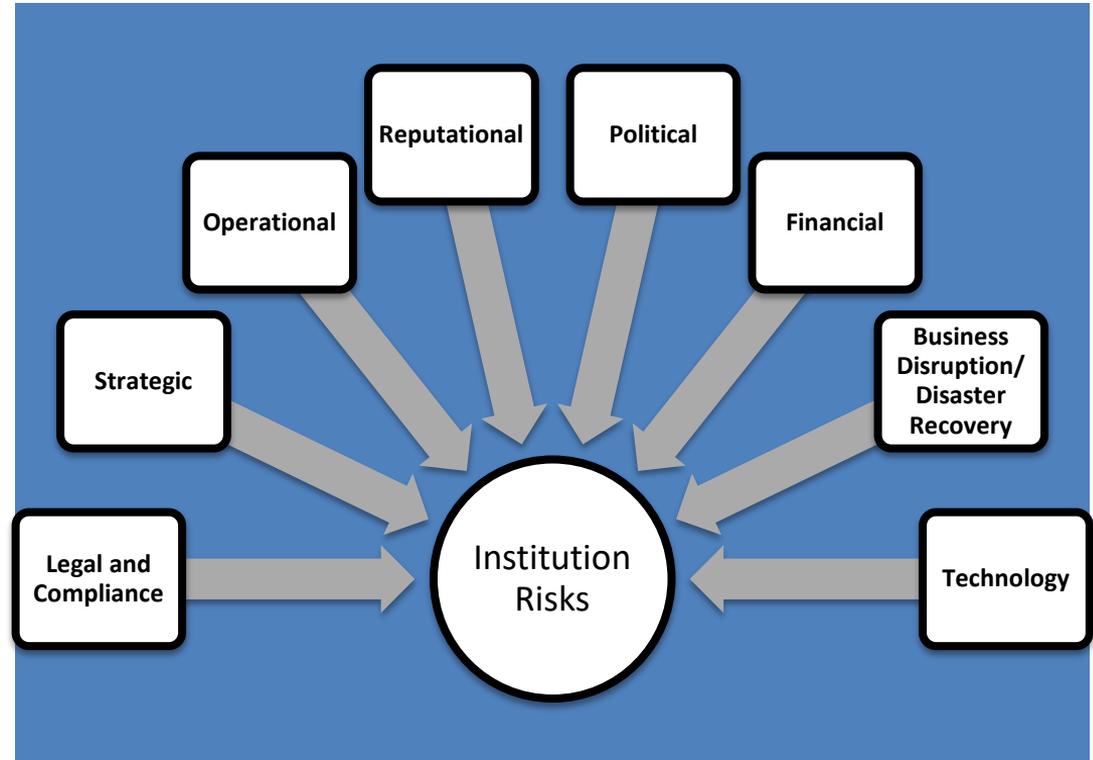
To improve cybersecurity risk knowledge and discuss management of cybersecurity risks



To improve fraud risk knowledge and discuss management of fraud risks



Critical risks across the institution have interdependencies and cannot be managed effectively in silos.

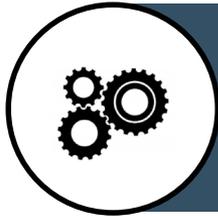




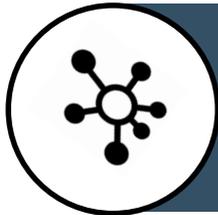
Enterprise Risk Management (ERM) and Institutional Leadership Context



Risk: The possibility that events will occur and affect the achievement of strategy and business objectives



Risk Management: A series of coordinated activities to direct and control challenges or threats to achieving an organizations goals



Enterprise Risk Management: The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value

What does ERM seek to do?

An organization-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos

Types of Risk



Financial

- Inaccurate, unreliable and/or incomplete financial statements and/or records
- Inadequate, ineffective and/or inappropriate internal controls



Reputation

- Inconsistent, inaccurate and/or inefficient administration, disbursement, and servicing of student aid
- Ineffective oversight and monitoring of Title IV programs and participants



Regulatory

- Failure to adhere to and/or implement requirements associated with Title IX/Clery Act
- Failure to resolve key control deficiencies identified during the audit process



Strategic

- Failure to achieve program targets
- Failure to achieve enrollment and retention targets
- Inability to perform significant academic or scientific research



Cyber

- Compromise of networks allowing unauthorized access to information
- Failure to protect personally identifiable information from unauthorized disclosure



While the Board of Trustees and President have ultimate accountability for managing risks and for achieving strategic objectives, risk management is everyone's responsibility.

Leading ERM and Strategy Realization: Questions for Consideration

- Does your institution have an ERM program?
- Do you focus on solving issues or managing critical risks?
- Are your key executives engaged in conversations about their units' risks and interdependencies?
- Are you engaged in risk conversations with your senior administrators and do those conversations involve risks tied to strategic objectives?
- Does your institution provide tools and training for risk management?
- Does your unit have a risk register and/or risk portfolio that feeds an institution-wide process?
- Has your institution assigned responsibility to a key executive to drive your institution-wide risk management process?
- Do you involve your entire organization in disciplined risk management?

Protecting Sensitive Data against Cybersecurity Threats

Mr. Wally Coy
CRISC, CISSP, CISM, CISA

First Some Definitions

From a cybersecurity perspective (i.e., Confidentially, Integrity, Availability of data, information, and/or information technology systems) the following definitions (based on NIST guidance) are generally accepted:

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Risk (Information Security Risk) - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

Risk Mitigation - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Cybersecurity Risks

The consequences of a cyber breach can include:

Compromised
Personally Identifiable
Information (PII)

Corrupt data such as
financial transactions and
academic records

Denial of access to critical
applications, systems, and
services

Enabling possible identity
theft and fraud scenarios

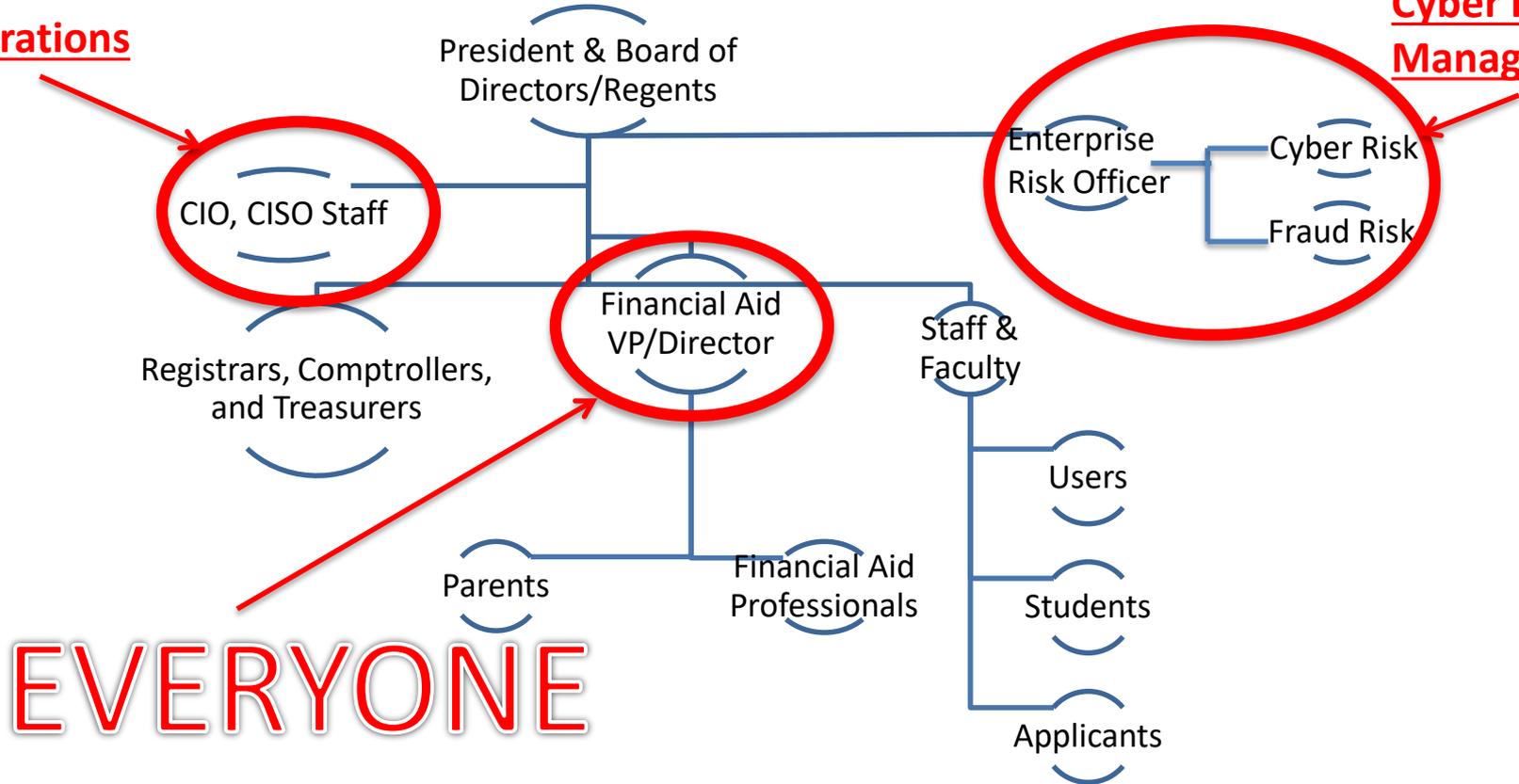
Potential reputational
damage to your institution

~ 90% of cybersecurity risks can be mitigated with good basic security controls or **“Cyber Hygiene” & User Education and Awareness**

Who is Responsible for Cyber Risk Management?

IT Operations

Cyber Risk Management

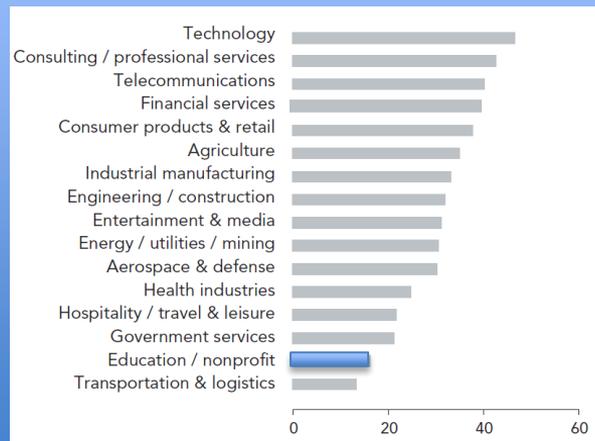


EVERYONE

Cybersecurity Challenges

The education sector tends to budget less for cybersecurity than most of the other sectors in our economy.

North American firms, by sector, with more than \$1 billion in gross revenue that budget \$10 Million or more for cybersecurity (percent)*



* Adapted from Office of Financial Research, Cybersecurity and Financial Stability: Risks and Resilience, February 15, 2017.

Top 5 Cyber Threat Vectors



Cyber threats most likely will exploit vulnerabilities associated with:

1. Human Behavior
2. Network Connectivity
3. Endpoint Devices
4. Authentication
5. App Stores

Top 5 Phishing Attacks



1. **Smishing** – phishing using SMS texts

2. **Spy-Phishing** – phishing using keyloggers

3. **Vishing** – phishing using phone calls

4. **Pharming** – phishing using redirection to fake websites

5. **Watering Hole Attacks** – phishing using typical websites used by targets (e.g. students, administrators, academic staff)

If They Can't Phish you . . .

they'll try to just guess your password! Vulnerabilities introduced by human behavior are the most likely to be exploited and password security is the most likely culprit.

New NIST “Digital Identity” guidelines* revise previous long-standing (and painful) password guidelines

- Less complex passwords
- Easy to remember longer “keyphases” with no preset expiration date
- Password hints and knowledge-based authentication (e.g., first pet) are **not** recommended
- 8 – 64 characters with all ASCII characters allowed
- 10 attempts before lockout
- Password checking against know password dictionaries

Instead of **G0T!gers#** use ***courage run spring play***, but many systems are not yet set up to allow such password so always follow your organizations security policy

The 25 most commonly used passwords of 2018**

1. 123456 (Unchanged)
2. password (Unchanged)
3. 123456789 (Up 5)
4. 12345678 (Down 1)
5. 12345 (Unchanged)
6. 111111 (New)
7. 1234567 (Up 1)
8. sunshine (New)
9. qwerty (Down 5)
10. iloveyou (Unchanged)
11. princess (New)
12. admin (Down 1)
15. welcome (Down 1)
14. 666666 (New)
15. abc123 (Unchanged)
16. football (Down 7)
17. 123123 (Unchanged)
18. monkey (Down 5)
19. 654321 (New)
20. !@#%* &* (New)
21. charlie (New)
22. aa123456 (New)
23. donald (New)
24. password1 (New)
25. qwerty123 (New)

* NIST Special Publication 800-63-3, Digital Identity Guidelines, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>

** <https://www.securitymagazine.com/articles/89919-the-25-passwords-leaked-online-in-2018>

Account Takeover (ATO) Attacks

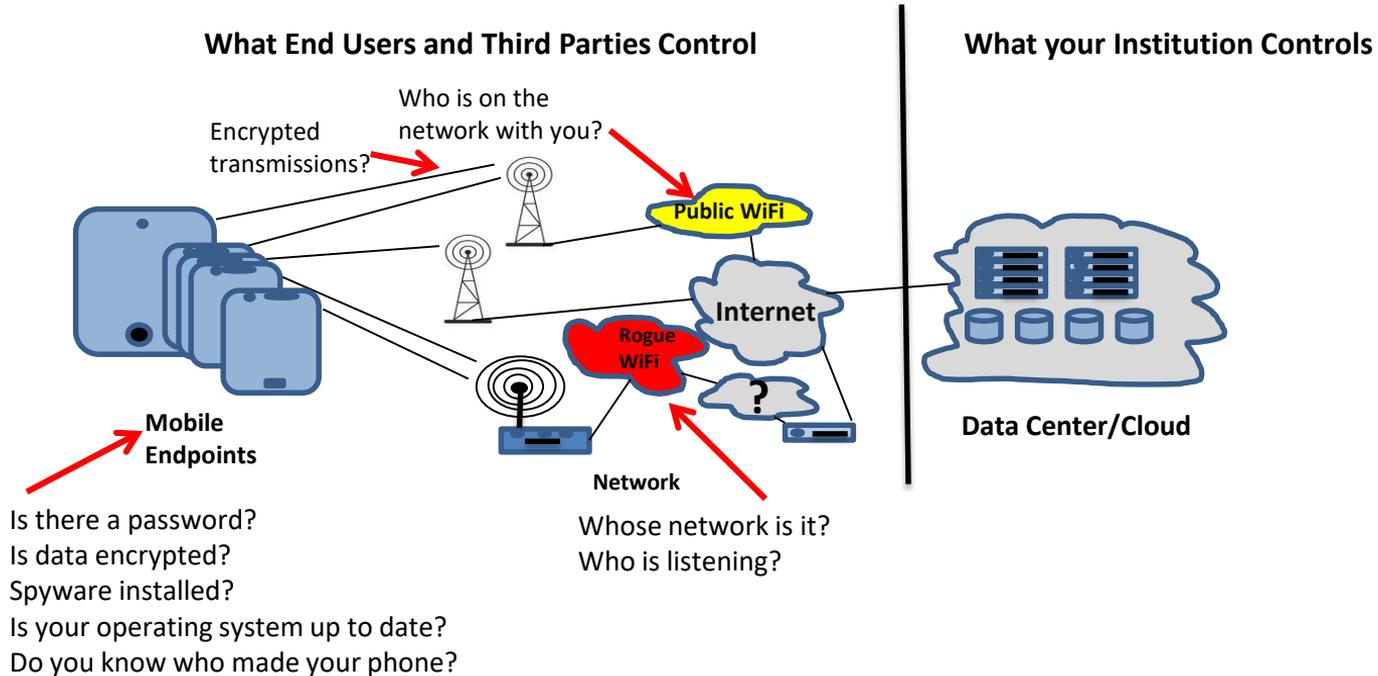
ATO attacks can be used to gain access to a user's email account (e.g., through phishing) and the attacker:

1. Establishes control of an account (persistence) without alerting the user or security administrators.
2. Conducts reconnaissance to determine how to exploit the account.
3. Exfiltrates sensitive information or steals funds and can repeat this process if user accounts credentials from other potentially higher-value targets were also compromised.

The attacker will potentially continue targeted email attacks and execute Business Email Compromise (BEC) and Vendor Email Compromise (VEC) to steal funds.

Mobile Endpoint Attack Surface

The primary cyber threat entry path is through endpoints your institution does not control (e.g., mobile phones, tablets, and personal computers).



Mobile User Behavior Vulnerabilities

Mobile User Behavior and Developer Practices Introduce Preventable Cybersecurity Vulnerabilities

For every 10,000 devices in an organization there is a ~95% chance that at least 1 device is infected with a malicious application that could be key stroke capture malware, ransomware, or other damaging spyware.*

50%

Do Not Use Passcodes

About half of mobile device users do not use passcodes to protect mobile devices which exposes the contents of the device if lost.

* Mobile Security Index 2019, Verizon

160

Unique IPs/Day

Mobile devices typically connect to an average of 160 unique IP addresses (Internet sites) a day potentially exposing devices to malicious sites and malware.

Mobile User Behavior Vulnerabilities (continued)

33%

Unencrypted

Over a third of mobile device communications is unencrypted potentially compromising PII of the user.

25%

**High Risk
Vulnerabilities**

A quarter of mobile applications have high risk security vulnerabilities that if exploited compromise the security of the device.

100%

Of Tested Apps

In a recent study of mobile banking applications all 30 apps analyzed had at least one security vulnerability which could result in the compromise of the device's security and users' data.

Cybersecurity Vulnerability Mitigation

Cyber Hygiene:

- Documented and enforced security policy and controls
 - Two-factor authentication for admins and critical applications
 - Testing your cybersecurity - vulnerability scanning and penetration testing
 - Incident Response Plans
 - Contingency Plans (Business Continuity Plans)
- & User Education and Awareness – especially for “phishing” attacks



BE PREPARED

Detecting, Responding, and Recovering from a Breach

How you detect, respond to, and recover from a cyber breach is as **(or more)** important than how you protect (i.e., through cyber hygiene) your systems

Intrusion Prevention/Detection Systems

- Endpoints (PC and mobile)
- Networks
- In the cloud

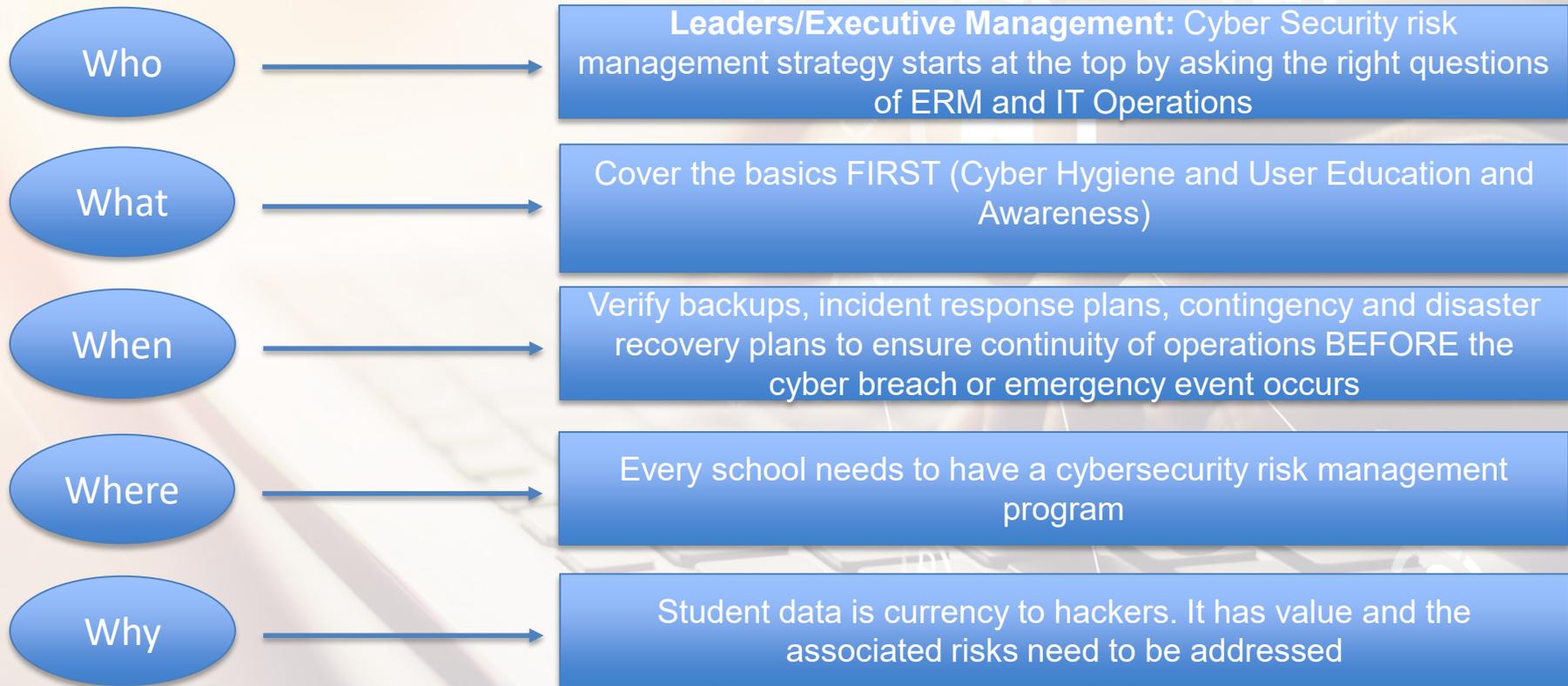
Incident Response Plans

- Policy
- Procedures
- Notification
- “Playbooks”
- “Tabletop Exercises”

Contingency Plans

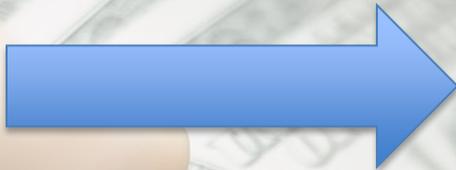
- Business Continuity Plans
- Disaster Recover Plan
- Backups
 - Local and offsite
 - Cloud-based backups
- Testing of backups

Closing Points

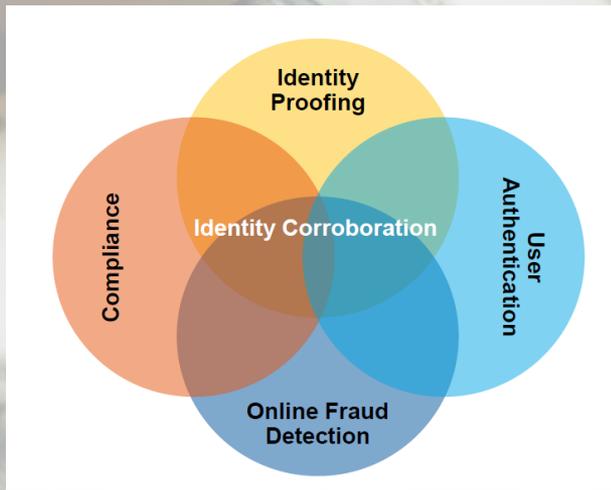


Cyber and Fraud Risk Management Work Together

Steal Data
“Cybercrime”



Steal Money
“Financial Crime”



Fraud Risk Management

Ms. Stephanie Powell

What is Fraud?

- **Financial**
- **Reward**
- **Acquired**
- **Using**
- **Deception**

“There is no kind of dishonesty into which otherwise good people more easily and frequently fall than that of defrauding the government.”

-Benjamin Franklin

We should manage fraud risk, but is it required?

**Under 34 CFR 668.16(g)(1)
MUST refer to OIG:**

- Applicant
- Administrator

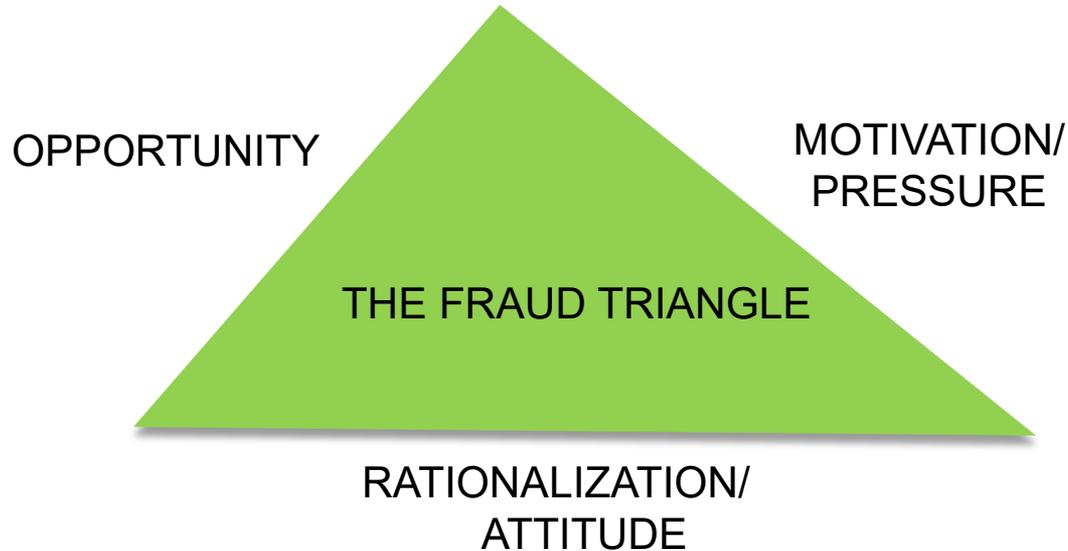
**if there is credible information
indicating fraud.**



Who may act fraudulently?



What risk factors may lead to fraud?



What is Fraud Risk Management?

Prevention



Detection



Start with Prevention



- ✓ Internal controls
- ✓ Separation of duties
- ✓ Retain and train staff
- ✓ Properly handle documents
- ✓ Shred sensitive information
- ✓ Use key identifiers-not SSN
- ✓ Password protection
- ✓ Review and audit access privileges
- ✓ Verify who you are talking with

Continue with a Focus on Detection



- ✓ **Review documents thoroughly**
- ✓ **Question documents/verify authenticity**
- ✓ **Request additional information**
- ✓ **Compare information on different documents**

Potential Red Flags for Detection

- ✓ Audits and repeat audit findings
- ✓ Unexplained entries in records
- ✓ Unusually large payments in cash
- ✓ Inadequate or missing documentation
- ✓ Altered records
- ✓ Non-serial number transactions
- ✓ Inventories and financial records not reconciled
- ✓ Unauthorized transactions
- ✓ Related Party Transaction
- ✓ FWS students' timecards exceed their free time
- ✓ Documentation from questionable sources or many from the same source
- ✓ "Students" being coached on what to say
- ✓ Inability to respond quickly to challenge questions
- ✓ Limited classroom activity
- ✓ Plagiarized and/or meaningless academic effort
- ✓ Just enough academic activity to generate a refund
- ✓ Multiple students with the same:
 - Physical and/or email address
 - Street and/or neighborhood/zip code
 - Home and/or cell phone number
 - IP address
 - Similar FAFSA®/ISIR information
 - Address change prior to disbursement

What happens when you detect fraud?

Call the professionals!!

Anyone suspecting fraud, waste, or abuse involving Department of Education funds or programs should call or write the Inspector General's Hotline.

1.800.MIS.USED

www.ed.gov/misused

Office of Inspector General
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202-1510

Differences Between OIG's Investigation Services and FSA's Program Compliance (PC) and Enforcement Offices (EO)

OIG INVESTIGATION SERVICES

Investigates any **fraud** impacting ED programs or operations

Works with federal and state prosecutors to take criminal and civil actions

Criminal investigators have statutory law enforcement authority to carry firearms and execute search and arrest warrants

Is independent of ED in exercising its investigative authority

FSA (PC AND EO)

Conducts compliance reviews, administrative investigations of violations of HEA

Takes administrative actions authorized by the HEA and program regulations

Reviewers and Investigators have administrative authority only

Has program operating responsibilities

Is required to send allegations of fraud to OIG



Contact Us

Dr. Michael Dean,
michael.dean@ed.gov
Deputy Chief Operating Officer

Ms. Kathy Zelnik, Kathy.Zelnik@ed.gov
Chief Risk Officer

Mr. Wally Coy, wallace.coy@ed.gov
Senior Advisor, Enterprise Cyber Risk

Ms. Stephanie Powell,
stephanie.powell@ed.gov
Senior Advisor, Fraud Risk

Questions and Answers