



Data Protection & Privacy

Cyber Breach Tabletop Exercise

Campus Resilience Program Exercise Starter Kit

October 23, 2018



FEMA



wcet



Office of
Academic
Engagement

Welcome and Introductions

Mike Abbiatti

Executive Director; WCET

Matt Johnson

Associate; Cooley, LLP

Cheryl Dowd

Cyber Fellow & SAN Director; WCET



FEMA



wcet



Office of
Academic
Engagement

Administrative Remarks

- Cell phone etiquette
- Evacuation procedures
- Restroom locations



FEMA



wcet



Office of
Academic
Engagement

Exercise Schedule

Activity	Time
Welcome and Data Protection Basics	9:00 a.m.
Exercise Overview	9:20 a.m.
Module 1: Initial Response	9:30 a.m.
TRANSITION TO MODULE 2	
Module 2: Extended Response	9:45 a.m.
Break	10:00 a.m.
Module 3: Short-Term Recovery	10:15 a.m.
Exercise Hot Wash	10:30 a.m.
Closing Remarks	10:40 a.m.



FEMA



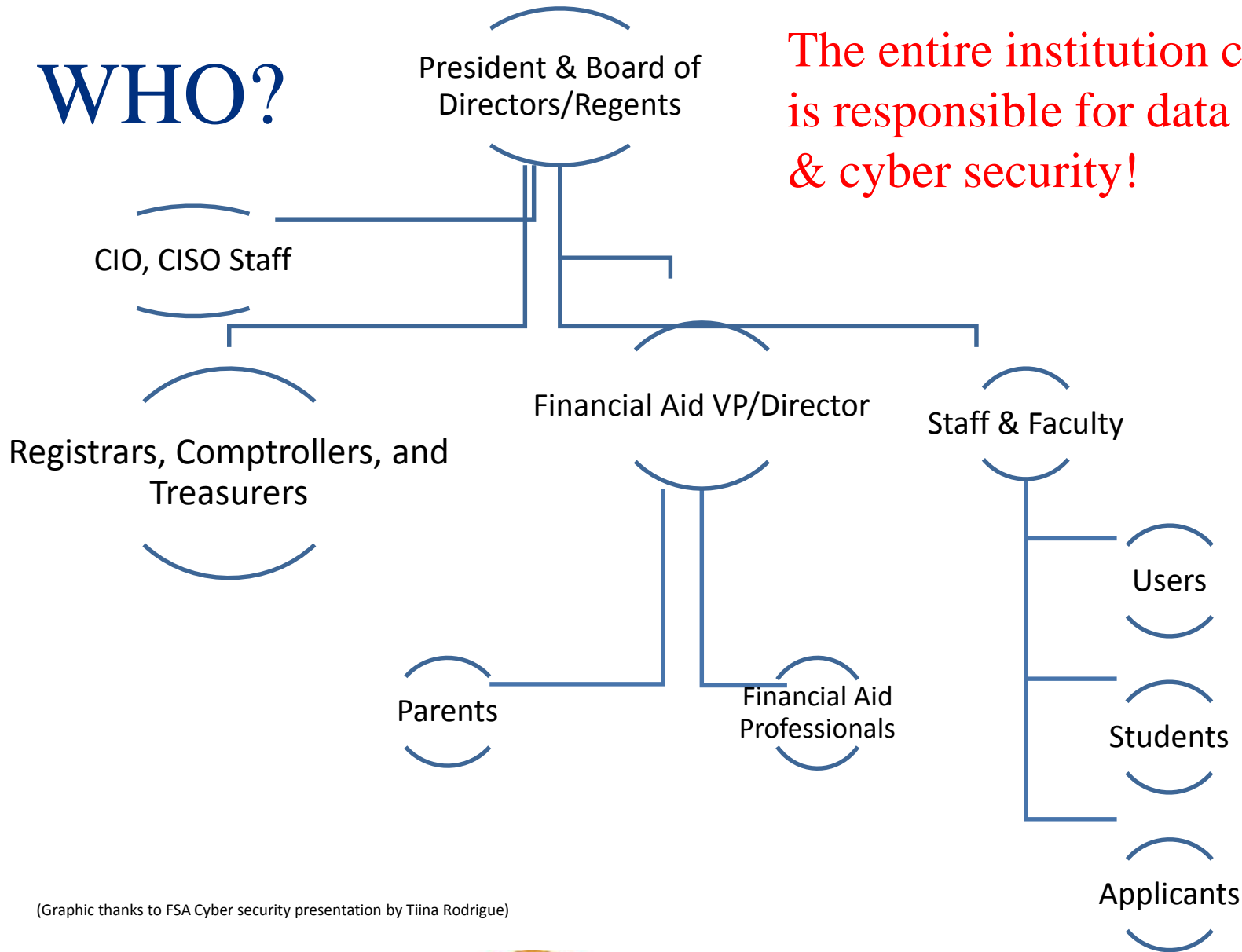
wcet



Office of
Academic
Engagement

WHO?

The entire institution community is responsible for data protection & cyber security!



(Graphic thanks to FSA Cyber security presentation by Tiina Rodrigue)



FEMA



wcet



Office of
Academic
Engagement

What?

Cyber Security = Computer Network Protection

- Data protection of the individual.
- Protection of the institution.
- More than just an IT issue!



FEMA



wcet



Office of
Academic
Engagement

What?

Cyber Security = Computer Network Protection

Vulnerable assets needing protection:

- Data collected on students, faculty, alumni and donors.
- Research data.
- Institutional Infrastructure.



FEMA



wcet



Office of
Academic
Engagement

WHY?



FEMA



wcet



Office of
Academic
Engagement

Cooley



Matt Johnson, Attorney

attorney advertisement

Copyright © Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304. The content of this packet is an introduction to Cooley LLP's capabilities and is not intended, by itself, to provide legal advice or create an attorney-client relationship. Prior results do not guarantee future outcome.

Gramm-Leach Bliley Act

- **Safeguard Rule**
 - FTC Enforcement
 - Applies to all institutions that receive financial aid (“financial institutions”)
 - Requirements:
 - Chief Privacy Officer
 - Risk Analysis
 - Comprehensive Governance Plan: technical, physical, administrative
 - Monitor, Test, Evaluate, Revise

Program Participation Agreement

- GLBA Compliance Required

“The Secretary considers any breach to the security of student records and information as a demonstration of a potential lack of administrative capability as stated in 34 CFR 668.16(c). Institutions are strongly encouraged to inform its students and the Department of any such breaches.”



State Data Breach Laws

- Breach notification laws in 47 states, D.C., Guam, Puerto Rico, Virgin Islands
- Based on where impacted person resides
 - Impact on distance ed program



Cost and Reputation

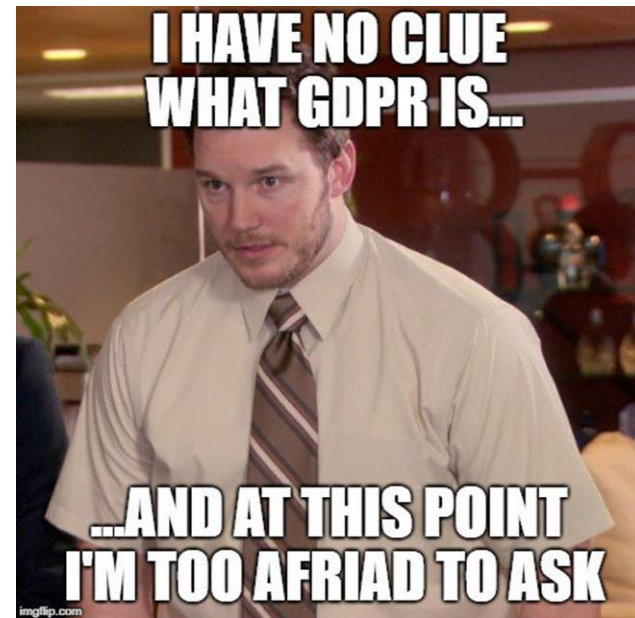
- Per Capita Cost Per Breach
 1. Healthcare
 2. Education → \$260 per compromised record
 3. Financial
 4. Pharmaceuticals



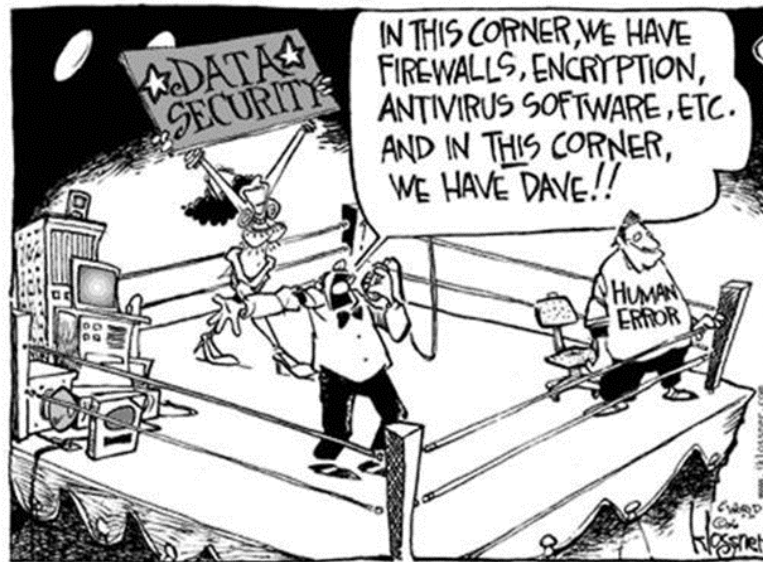
Four Year Global Average *IBM Ponemon Institute Study (2017)*

GDPR – So Much to Discuss, So Little Time

- Jurisdiction over entities *established* in the EU and those offering its citizens or residents goods/services or monitoring them.



Training is Key



Everyone has a Dave.

Questions?

mjohnson@cooley.com

Cooley

Exercise Overview



FEMA



wcet



Office of
Academic
Engagement

Exercise Overview

Background:

- This Tabletop Exercise (TTX) is made available through the Campus Resilience (CR) Program Exercise Starter Kits
- Each Exercise Starter Kit aims to support practitioners and senior leaders from the academic community in assessing emergency plans, policies, and procedures while also enhancing overall campus resilience

Purpose:

- This specific Exercise Starter Kit will provide the opportunity to examine response and recovery operations related to cyber breach targeted against institutional data



FEMA



wcet



Office of
Academic
Engagement

Exercise Overview (cont.)

Scope:

- This two-hour TTX is divided into three Modules:
 - **Module 1** will examine immediate response operations four hours following the initial notification of a cyber breach
 - **Module 2** will examine extended response operations up to 36 hours following the notification of a cyber breach
 - **Module 3** will examine short-term recovery operations seven days following the notification of a cyber breach
- Each Module will consist of two activities:
 1. **Scenario Overview:** Each Module will contain a detailed overview of the scenario
 2. **Facilitated Discussions:** Participants will engage in facilitated discussions surrounding a set of discussion questions



FEMA



wcet



Office of
Academic
Engagement

Exercise Objectives

1. **Operational Coordination:** Assess the ability to establish an effective command structure that integrates all critical stakeholders to ensure campus and community resources are used efficiently to respond to and recover from a cyber incident
2. **Cybersecurity:** Evaluate existing capabilities to protect and restore electronic systems, networks, information, and services from damage, unauthorized use, and exploitation during a cyber incident
3. **Situational Awareness:** Examine the ability to provide timely and relevant information regarding the cyber incident to critical campus and community decision-makers
4. **Public Information and Warning:** Assess the ability to deliver coordinated, actionable, and timely information to critical partners and stakeholders when faced with a cyber incident targeting institutional operations



FEMA



wcet



Office of
Academic
Engagement

Participant Roles and Responsibilities

- **Facilitator:** Provides situation updates and facilitates discussions
- **Players:** Respond to the situation presented based on current plans, policies, and procedures
- **Observers:** Visit or view selected segments of the exercise without directly engaging in exercise discussions
- **Support Staff:** Performs administrative and logistical support during the exercise (e.g., registration)



FEMA



wcet



Office of
Academic
Engagement

Exercise Guidelines

- This exercise is being conducted in an **open, low-stress, no-fault environment**; varying viewpoints, even disagreements, are expected
- Act in real-world roles for your institution or organization when considering the scenario
- Decisions are **not precedent-setting**; this is an open discussion
- The focus should be on **identifying suggestions and recommended actions** for improving preparedness, response, and recovery efforts



FEMA



wcet



Office of
Academic
Engagement

Assumptions and Artificialities

- The exercise **scenario is plausible** and events occur as they are presented
- Players will use **existing plans, policies, procedures, and resources** to guide responses
- There is **no “hidden agenda”** nor are there any trick questions
- The scenario assumes certain player actions as it moves through each phase; players should first discuss the actions stipulated by the scenario
- Players are welcome to engage in **“what if” discussions** of alternative scenario conditions



FEMA



wcet



Office of
Academic
Engagement

Start of Exercise



FEMA



wcet



Office of
Academic
Engagement

Module 1: Initial Response



FEMA



wcet



Office of
Academic
Engagement

Module 1: Background

- In recent years, malicious cyber actors have targeted colleges and universities with cybercrime activities
- An additional emerging threat facing institutions of higher education includes cyber espionage in an attempt to gain access to scientific and medical research as well as potentially sensitive government and private-sector research information
- College and university networks may present an easier target for cyber espionage actors due to multiple levels of connectivity and accessibility
- Furthermore, they present an easier target due to lower cyber security awareness among students, faculty, and staff



FEMA



wcet



Office of
Academic
Engagement

Module 1: Scenario Overview

October 26, 2018 10:00 am

- Your institution's Chief Information Security Officer is contacted by a Special Agent from the Cyber Division at the FBI
- The agent states that a cyber attack has been launched against your institution's network by an outside entity and currently the duration, scope, and source of the attack is not clear
- An initial investigation reveals the presence of an advanced persistent threat (APT) that appears to be consistent with malware known to be associated with other university attacks



FEMA



wcet

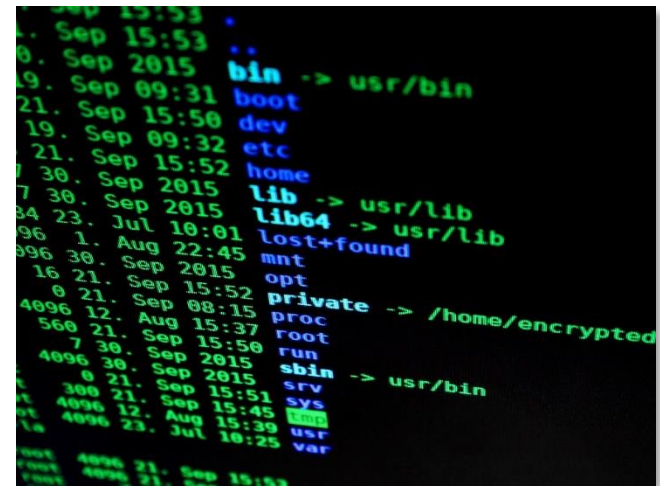


Office of
Academic
Engagement

Module 1: Scenario Overview (cont.)

October 26, 2018 2:00 pm

- By this time, evidence determines the attack was initiated three months prior, providing attackers with unlimited access to networks, databases, servers, and other sensitive resources associated with various departments and colleges
- While exfiltration of data cannot be confirmed, it is reasonable to assume that sensitive information has been compromised
- A thorough analysis of the entire institution network has been initiated but may take a day or more to complete



FEMA



wcet



Office of
Academic
Engagement

Module 1: Discussion Questions (1/4)

Operational Coordination

1. What plans, policies, and procedures does your institution have in place to respond to the effects of a data breach?
2. What are your institution's initial priorities?
3. How would your institution establish a command structure to coordinate your immediate response efforts?
4. What resource gaps could limit your institution's ability to respond to a cyber attack?



FEMA



wcet



Office of
Academic
Engagement

Module 1: Discussion Questions (2/4)

Cybersecurity

1. Does your institution have a formalized cyber incident response plan?
2. Does your institution's response strategy outline how to align broader response efforts with ongoing security management and IT efforts?
3. What steps will your institution take to verify the likelihood of a data breach resulting in the release of PII?
4. What measures are in place to protect confidential, personal, financial, and academic information concerning students, faculty, staff, and alumni from a potential cyber incident?



FEMA



wcet



Office of
Academic
Engagement

Module 1: Discussion Questions (3/4)

Situational Assessment

1. How does your institution collect, verify, and analyze information immediately following awareness of, or notification of a cyber incident?
2. How do you conduct initial decision-making and offer decision-making recommendations to senior leadership?
3. Do you have identified information requirements that support leadership decision-making processes (e.g., type of cyber incident, scope of incident, numbers of individuals impacted, implementation of cyber response plan)?



FEMA



wcet



Office of
Academic
Engagement

Module 1: Discussion Questions (4/4)

Public Information and Warning

1. What plans, policies, and procedures does your institution have in place to guide communications with potentially affected parties at this time?
2. What individual, office, or department coordinates and delivers your institution's messaging?
3. How will your institution use social media platforms in support of incident communications and messaging?
4. At this point in the scenario, would your institution notify non-affected members of the campus community?



FEMA



wcet



Office of
Academic
Engagement

Module 2: Extended Response



FEMA



wcet



Office of
Academic
Engagement

Module 2: Scenario Overview

October 26, 2018 10:00 pm

- A second intrusion has been detected on your institution's network
- During the investigation, a malware variant used to exfiltrate personally identifiable information was discovered on several computers in the Office of Human Resources, the Admissions and Registration Offices, and the Financial Aid and Scholarship Offices

October 27, 2018 10:00 am

- A detailed review of internal logging systems indicates stolen employee login credentials may have been used to access databases containing both student and faculty records
- Data appears to have been exfiltrated over several months



FEMA



wcet



Office of
Academic
Engagement

Module 2: Scenario Overview (cont.)

October 27, 2018 10:00pm

- Local news outlets begin contacting your public affairs office in response to reports that a data breach has occurred at your institution
- Reporters note that they have heard that the personal information of hundreds of students, faculty, and staff has been stolen and are requesting more information on the situation
- Students and parents begin contacting your IT department expressing concerns over their personal information



FEMA



wcet



Office of
Academic
Engagement

Module 2: Discussion Questions (1/4)

Operational Coordination

1. What plans, policies, and procedures does your institution have in place to guide response efforts at this point?
2. How would your institution maintain an effective command structure to coordinate cyber response efforts?
3. How do key decision-makers collect information on system damages and critical needs?
4. What resources are currently available to support response efforts?
5. Who are the key external stakeholders that would support response efforts?



FEMA



wcet



Office of
Academic
Engagement

Module 2: Discussion Questions (2/4)

Cybersecurity

1. What tools are in place to prevent the remote extraction of information from a network by unauthorized users?
2. Do you currently possess sufficient capabilities in-house to investigate and mitigate a potential incident of this type?
3. What types of impacts could your institution expect from the potential loss of PII?
4. What plans, policies, and procedures exist to ensure students, faculty, and staff engage in information security best practices?



FEMA



wcet



Office of
Academic
Engagement

Module 2: Discussion Questions (3/4)

Situational Assessment

1. Have your information needs changed during this phase of the response?
2. What are the processes for communication and coordination between internal and external partners to support any emerging needs or response requirements?
3. Are there identified reporting requirements for internal stakeholders? For external partners? For leadership and key decision-makers?



FEMA



wcet



Office of
Academic
Engagement

Module 2: Discussion Questions (4/4)

Public Information and Warning

1. At this point in the scenario, how would your institution be communicating with potentially affected as well as non-affected parties?
2. How does your institution ensure timely and accurate situational updates for external stakeholders (e.g., media) throughout the response period?
3. Does your institution have a crisis communications plan or other means of communicating with all stakeholders in case of a disruption or corruption of standard communications?



FEMA



wcet



Office of
Academic
Engagement

Break



FEMA



wcet



Office of
Academic
Engagement

Module 3: Short-Term Recovery



FEMA



wcet



Office of
Academic
Engagement

Module 3: Scenario Overview

November 2, 2018 10:00am

- A full analysis of the entire network reveals that the scope of the data breach is more extensive than previously suspected
- Health-related data and donor information appears to have also been compromised
- Students, faculty, and staff express concerns over their personal information and inquire about what your institution is doing to protect their data
- Media outlets reporting on the breach highlight stories criticizing the way your institution handled the situation



FEMA



wcet



Office of
Academic
Engagement

Module 3: Discussion Questions (1/4)

Operational Coordination

1. How does your institution coordinate the transition from response to short-term recovery efforts?
2. What plans, policies, and procedures guide your institution's recovery process?
3. What resource gaps could limit your institution's ability to meet these priorities?



FEMA



wcet



Office of
Academic
Engagement

Module 3: Discussion Questions (2/4)

Cybersecurity

1. What partnerships does your institution have to support recovery efforts (e.g., cyber insurance) in the aftermath of a cyber incident?
2. What are your institution's plans for the recovery and restoration of critical systems and data that have been compromised as a result of a cyber related incident?
3. What strategies would be implemented to mitigate potential negative impacts resulting from stolen and/or leaked PII?
4. What future cybersecurity measures could you implement to develop more secure systems and protect critical institutional data from a future breach?



FEMA



wcet



Office of
Academic
Engagement

Module 3: Discussion Questions (3/4)

Situational Assessment

1. What critical decisions would need to be made at this point to inform recovery efforts?
2. What legal obligations exist, if any, that may affect how intelligence and information is processed and communicated following a cyber related incident?
3. Following this type of incident, what decisions or actions would you take to maintain public and institutional confidence?



FEMA



wcet



Office of
Academic
Engagement

Module 3: Discussion Questions (4/4)

Public Information and Warning

1. How does your institution ensure consistent, coordinated public messaging throughout the recovery period?
2. How does your institution provide external stakeholders (e.g., media) with timely updates concerning recovery efforts?
3. How would you maintain overall brand reputation for an incident involving a cyber breach?
4. How are students, faculty, and staff briefed on protective actions and measures to prevent future cyber incidents?



FEMA



wcet



Office of
Academic
Engagement

End of Exercise



FEMA



wcet



Office of
Academic
Engagement

Exercise Hot Wash



FEMA



wcet



Office of
Academic
Engagement

Hot Wash Overview

- This Hot Wash aims to capture the following information based on observations made throughout the exercise:
 - Overall strengths
 - Overall areas for improvement
 - Major takeaways and action items



FEMA



wcet



Office of
Academic
Engagement

HOW?

Practical Steps

- Create an institution compliance & data risk mitigation plan.
- Designate a person responsible for data protection policy compliance.
- Provide training to all staff on information security.
- Develop an incident response plan that includes Backup and Disaster Recovery System.
- Know and prioritize institutional assets to know how they are to be protected.



FEMA



wcet



Office of
Academic
Engagement

HOW?

Points to Remember:

- Plan & Prepare!
- Test your plans.
- Security = Absence of un-mitigatable surprise.



FEMA



wcet



Office of
Academic
Engagement

What are WCET and WICHE Doing?

1. Developed relationship with DHS to provide LTTX in WICHE states.
2. Creating relationships and attending training events with the NCC.
3. Developing a WICHE Data Governance Plan that is GDPR compliant.
4. WCET Issue Page: Data Protection and Privacy

<https://wcet.wiche.edu/focus-areas/policy-and-regulation/data-protection-privacy>



FEMA



wcet



Office of
Academic
Engagement

Adjournment



FEMA



wcet



Office of
Academic
Engagement