

Community Cybersecurity Preparedness Simulation

Everyone has a role

CTAO Conference
May 2024

Natalie Sjelin
Director Training, CIAS



FEMA



Course Development



This course was developed by
The Center for Infrastructure Assurance and Security
At The University of Texas at San Antonio

The CIAS has been working with communities to improve their cybersecurity posture since 2002.

Core competencies include cybersecurity training, exercises, competitions, game development, culture of security initiatives, information sharing and cybersecurity community programs.



Consortium Members

- National Cybersecurity Preparedness Consortium Members
 - Cyber Defense Initiative-CJI/UA System
 - Center for Infrastructure Assurance and Security-University of Texas-San Antonio
 - Texas A&M Engineering Extension Service-Texas A&M University System
 - Center for Information Assurance, Univ. Memphis
 - Norwich University Applied Research Institutes, Norwich University

National Cybersecurity Preparedness Consortium



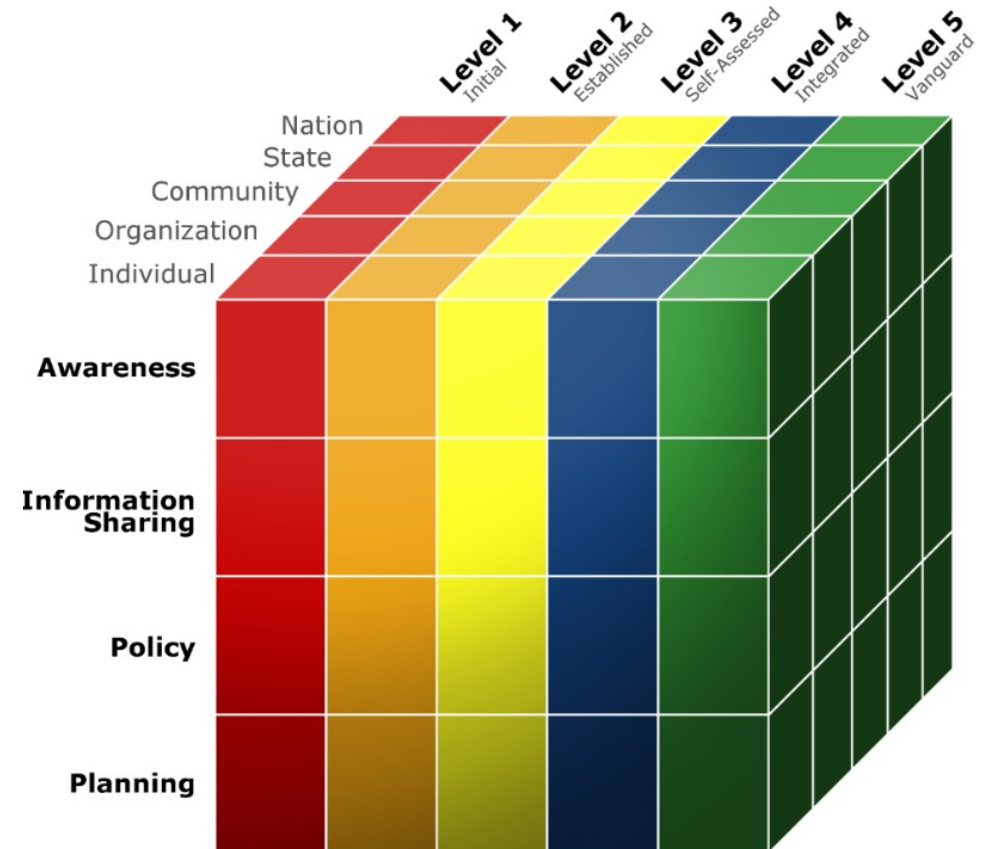
FEMA



Organized Around the CCSMM

The Community Cyber Security Maturity Model:

- Framework for cybersecurity preparedness
 - Focusing first on low and no cost solutions
- Everyone has a role in cybersecurity from the individual, organization, community, state and nation
- Addresses all aspects of cybersecurity
- Incorporates other frameworks such as the NIST CSF, NICE, CMMC, EMP and others
- Provides a roadmap to improve cybersecurity posture



FEMA



MGT-301 Community Cybersecurity Preparedness Simulation

- This one-day course is designed to simulate a community-wide cybersecurity event.
- Using a gamification approach, participants will strategize with a diverse group of stakeholders to plan for and respond from a cybersecurity incident that could have cascading effects across a community.



FEMA



Objectives

- Discuss organizational and community cybersecurity preparedness
- Explain how budgeting and planning considerations with limited resources play a role in a cybersecurity program
- Discuss possible cascading effects a cyber-attack may have on a community
- Identify strategies to prevent, detect, mitigate, respond to, and recover from a cyber incident



FEMA



Cyber-attacks on Communities

- Atlanta, Ga.
- Baltimore, Md.
- St. Lucie, Fla.
- New Bedford, Mass.
- New Orleans, La.
- Greenville, N.C.
- Pensacola, Fla.
- Wilmer, Texas
- And more...



FEMA



Cyber-attacks in Ohio

- **Riverside (May 2018)**
 - Police and Fire Departments 2 attacks within weeks. Deleted 10 months of information
- **Lakeland Community College (Sep 2023)**
- **City of Circleville (Sept 2023)**
- **Huber Heights (Nov 2023)**
 - Compromised PII 6,000 people. Affected the city's zoning, engineering, tax, fiancé, utilities, human resources, and economic development divisions.
- **Healthcare (Feb 2024)**
 - Change Healthcare – unable to process claims
 - Arlington Health – unable to submit patient bills



FEMA



Community Vulnerability Landscape

The convergence of physical and information technologies used by communities create new opportunities for cyber-attacks. Some key technologies and systems:

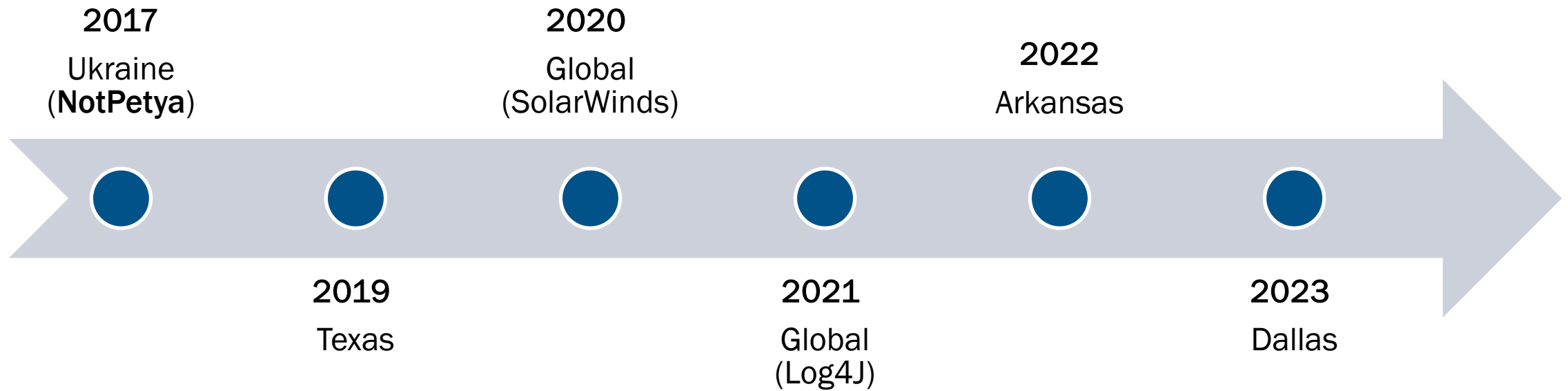
- Traffic Control Systems
- Smart Street Lighting
- Regional Utility Management Systems (electric, waste, water)
- Sensors
- Public Data
- Mobile Applications
- Cloud and SaaS Solutions
- Smart Grid
- Public Transportation
- Cameras
- Social Media
- Location-based Services



FEMA



Cascading and Widespread Impacts Over Time



FEMA



Adversary Motives (Why)



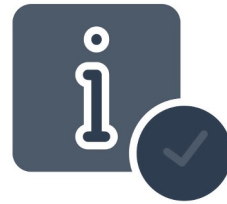
Financial



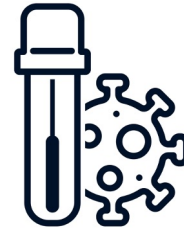
War or
Defense



Social or
Political



Facilitation



Nuisance or
Destruction



Ego



Espionage



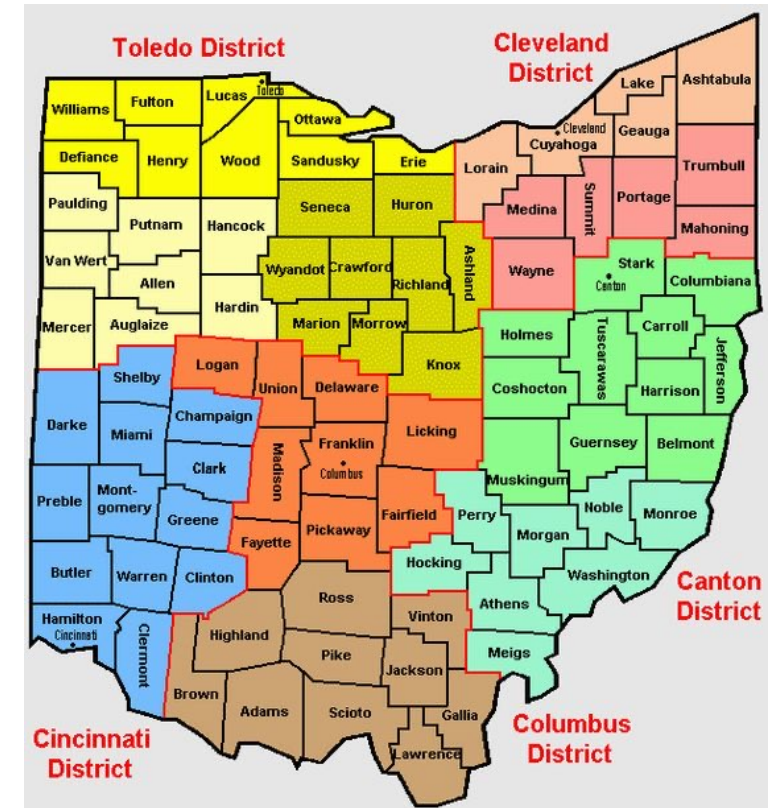
FEMA



Ohio County Treasurers Role

Ohio County Treasurers Responsibilities

- Tax collection: Collecting local taxes
- Tax safekeeping: Safeguarding taxes for schools, cities, townships, and villages
- Financial statement preparation
- Fund investment
- Cash management: County's cash manager and leader in fiscal management and accountability
- Delinquent tax collection
- Property tax escrow account
- Unclaimed funds



FEMA



Mission Essential Functions (Critical Business Services)

Mission Essential Functions

Mission Essential Functions (MEFs) are a limited set of functions that must be continued throughout or resumed rapidly following the disruption of normal operations. Enable organizations to provide vital services, such as:

- Exercise civil authority
- Maintain public health & safety
- Sustain critical economic activities
- Uphold the rule of law



FEMA

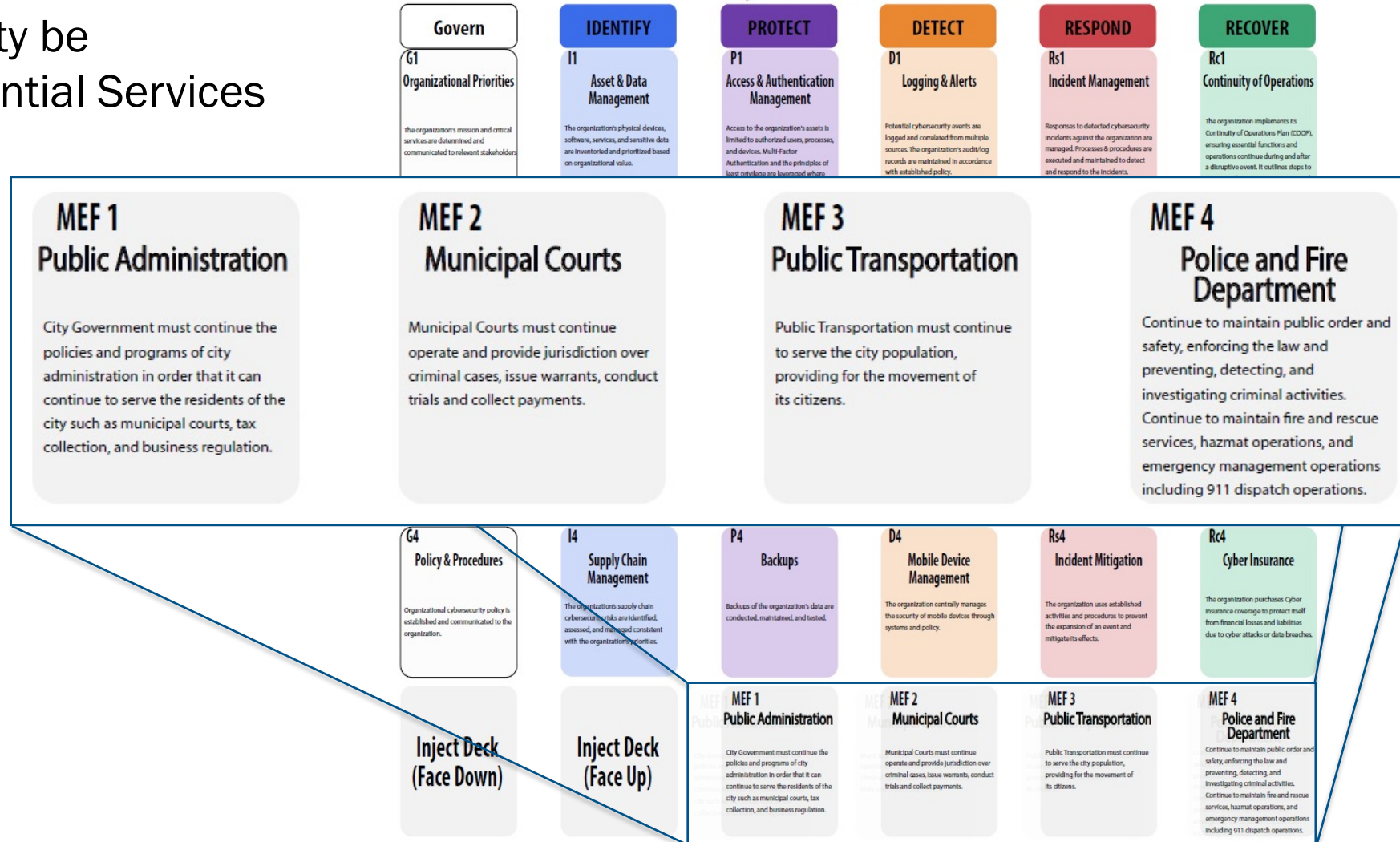


Organizational MEFs vs Community Resilience

How would the community be impacted if Mission Essential Services were compromised?

- City Government
- City Utilities
- Community Bank
- Community Hospital
- K-12 School District
- Private Sector Business

City Government



FEMA

Treasurer Essential Functions

How would the community be impacted if your Mission Essential Services were compromised?

- Collect Tax Payments
- Receive monies from county offices
- Distribute/Manage ACH's
- Balance daily work
- Monitor and Move Investments
- Tax Bill Prep and mail
- Month End Reports
- Tax Ease Certs



FEMA

City Government



Organizational Cybersecurity Budgeting & Planning

Cybersecurity Budgeting and Planning

Leaders need to think about how much funding they will need, and how they will allocate their budgets to address cybersecurity threats their organizations may face.

Key factors:

- Need to know what to protect.
- Need to have methods to detect and respond.
- Need to have a cyber-recovery plan in place.
- Need to educate and train your employees regularly.



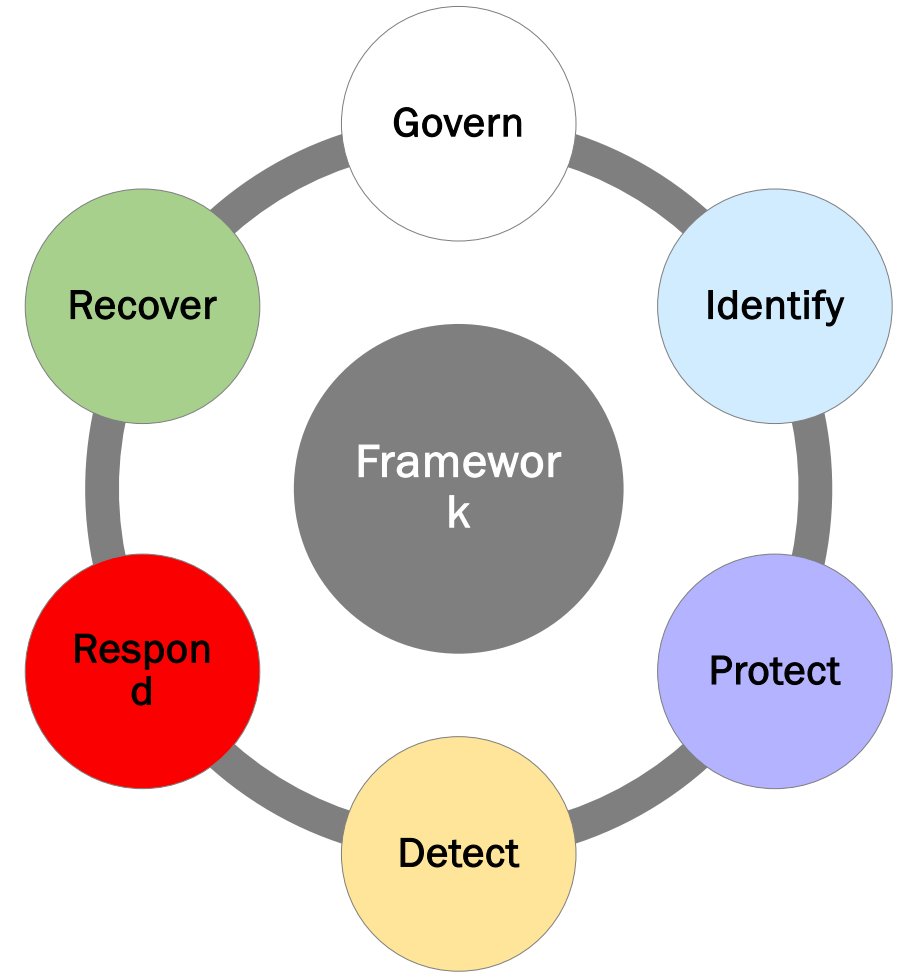
FEMA



NIST Cybersecurity Framework (CSF)

The NIST CSF is:

- A living document based on international standards.
- A common and accessible language.
- Risk-based.
- Adopted internationally.
- Used in the Nationwide Cybersecurity Review.
- Leveraged by public and private entities.



FEMA



The Cybersecurity Planning Board

- The planning board is a matrix depicting an **Organization's Cybersecurity Planning Framework**:
 - categories are **Govern, Identify, Protect, Detect, Respond** and **Recover**.
- Each category of the Framework is divided into smaller **subcategories**, representing cybersecurity actions and controls.
- Displayed are the top four Mission Essential Functions (MEFs) for the organization.



FEMA

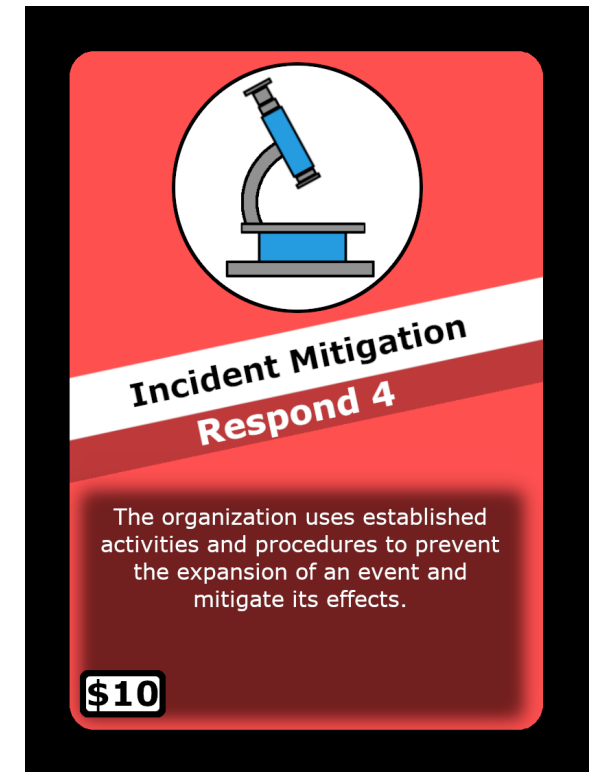
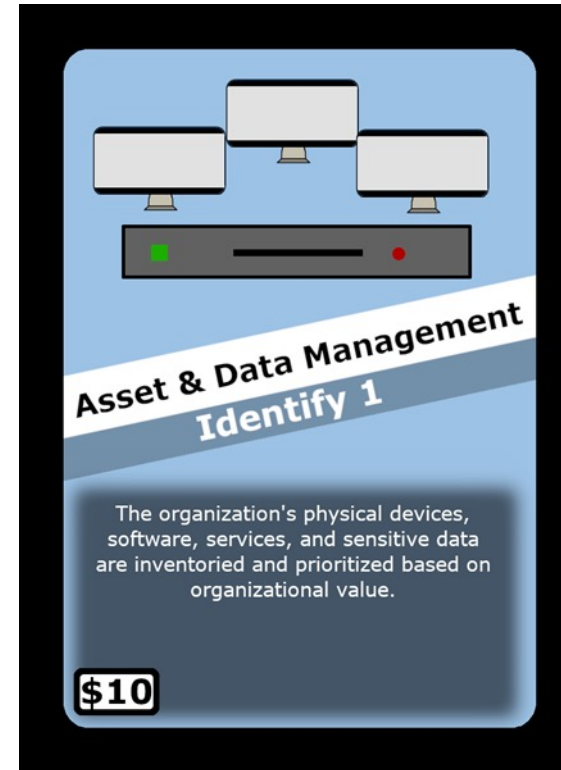


The Organization's Planning Cards

Each planning group has 24 planning cards that correspond to the subcategories on the planning board.

Each planning card features a:

- Subcategory name
- Identifying number (e.g., Identify 1)
- Description of the actions or controls
- Budget cost



FEMA



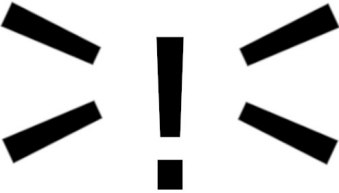
Planning Cards – Govern



Organizational Priorities
Govern 1

The organization's mission and critical services are determined and communicated to relevant stakeholders.


\$5



Risk Management
Govern 2

The organization's Risk Management processes are established, managed, and agreed to by organizational stakeholders.


\$5



Roles and Responsibilities
Govern 3

Cybersecurity roles are integrated into human resources practices, and responsibilities are coordinated and aligned with all internal and external stakeholders to enable accountability, performance assessment, and continuous improvement.

\$5



Policy Plan Procedure

Policy and Procedures
Govern 4

Organizational cybersecurity policy is established and communicated to the organization.

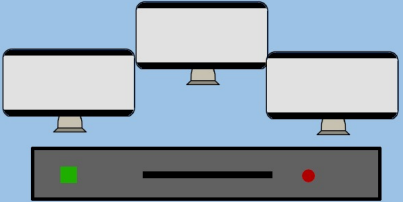
\$5



FEMA



Planning Cards – Identify



Asset & Data Management
Identify 1

The organization's physical devices, software, services, and sensitive data are inventoried and prioritized based on organizational value.


\$10



Vulnerability Management
Identify 2

The organization's processes and procedures for receiving, validating, and responding to vulnerabilities are defined. Vulnerability scans are performed.

\$15



Information Sharing - Collection
Identify 3

Cyber threat intelligence is received from information sharing organizations (ISAOs), forums, and other sources.

\$10



Supply Chain Management
Identify 4

The organization's supply chain cybersecurity risks are identified, assessed, and managed consistent with the organization's priorities.

\$10



FEMA



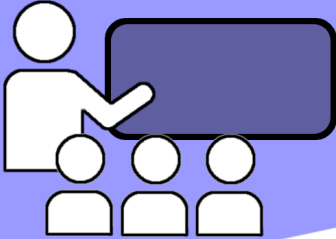
Planning Cards – Protect



Access & Authentication
Protect 1

Access to the organization's assets is limited to authorized users, processes, and devices. Multi-Factor Authentication and the principles of least privilege are leveraged where risks of unauthorized access are high.

\$10



Awareness & Training
Protect 2

The organization's employees and partners receive training on cybersecurity awareness, duties, and responsibilities according to policies, procedures, and agreements.


\$5



Encryption
Protect 3

The confidentiality, integrity, and availability of the organization's data at rest, in use, and in transit are protected.

\$5



Backups
Protect 4

Backups of the organization's data are conducted, maintained, and tested.

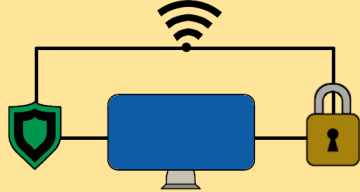
\$10



FEMA



Planning Cards – Detect



Logging and Alerts
Detect 1

Potential cybersecurity events are logged and correlated from multiple sources. The organization's audit/log records are maintained in accordance with established policy.

\$10



Network Monitoring
Detect 2

The organization's networks and network services are monitored for adverse cybersecurity events.

\$10



Virus Protection
Detect 3

The organization uses antivirus software to protect against cybersecurity malware threats.

\$5



Mobile Device Management
Detect 4

The organization centrally manages the security of mobile devices through systems and policy.

\$5



FEMA




Planning Cards – Respond



**Incident Management
Respond 1**

Responses to detected cybersecurity incidents against the organization are managed. Processes & procedures are executed and maintained to detect and respond to the incidents.


\$15



**Incident Analysis
Respond 2**

The organization conducts investigations of cybersecurity events to ensure effective responses and support recovery activities.


\$10



**Incident Reporting & Communication
Respond 3**

The organization coordinates information sharing and escalation procedures with designated internal and external stakeholders (such as Federal, State & law enforcement agencies) as required by law, regulation, or policy.

\$10



**Incident Mitigation
Respond 4**

The organization uses established activities and procedures to prevent the expansion of an event and mitigate its effects.

\$10



FEMA



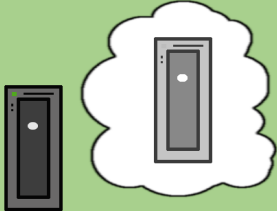
Planning Cards – Recover

PLAN
B

**Continuity of Operations
Recovery 1**

The organization implements its Continuity of Operations Plan (COOP), ensuring essential functions and operations continue during and after a disruptive event. It outlines steps to minimize downtime, maintain critical services, and recover promptly.

\$10



**Systems and Data Recovery
Recovery 2**

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.


\$10

Why Where
Who
How What
When

**Public Relations
Recovery 3**

The organization communicates its recovery activities and progress in restoring operational capabilities with relevant internal and external stakeholders.

\$5



**Cyber Insurance
Recovery 4**

The organization purchases Cyber Insurance coverage to protect itself from financial losses and liabilities due to cyber attacks or data breaches.

\$15



FEMA



The Organization's Planning Budget

The Cyber Program Budget is **\$100**.

- Purchase Planning Cards
 - Represents implementation of the controls/activities
 - Uncovered areas are not being performed or implemented
- Record on Budget Planning Tracking Sheet

Budget Planning Tracking Sheet

Planning Card Title	Cost	Purchasing Budget Used
		(\$100 allowed)
G1 Organizational Priorities	\$5	
G2 Risk Management	\$5	
G3 Roles & Responsibilities	\$5	
G4 Policy & Procedures	\$5	
I1 Asset & Data Management	\$10	
I2 Vulnerability Management	\$15	
I3 Information Sharing - Collection	\$10	
I4 Supply Chain Management	\$10	
P1 Access & Authentication	\$10	
P2 Awareness & Training	\$5	
P3 Encryption	\$5	
P4 Backups	\$10	
D1 Logging & Alerts	\$10	
D2 Network Monitoring	\$10	
D3 Virus Protection	\$5	
D4 Mobile Device Management	\$5	
Rs1 Incident Management	\$15	
Rs2 Incident Analysis	\$10	
Rs3 Incident Reporting & Communication	\$10	
Rs4 Incident Mitigation	\$10	
Rc1 Continuity of Operations	\$10	
Rc2 System & Data Recovery	\$10	
Rc3 Public Relations	\$5	
Rc4 Cyber Insurance	\$15	
Total Planning Budget Used (\$100 allowed)		

* Costs are based on Talent, Technology, and Time considerations.



FEMA



Activity – Organizational Planning (15 Min)

1. In your group, review the planning cards.
2. Your organization has a budget of \$100 to spend on cybersecurity.
3. Discuss the activities you deem most important.
4. Select the planning cards your organization will purchase:
 - track purchases on the Budget Planning Tracking Sheet; and
 - stay within your budget.
5. Cover the activities you purchased on the Planning Board with the Planning Card.
6. Select a Reporter and Score Keeper.
7. Consider the following questions. Be prepared to share your observations:
 - Which 2-3 activities are most important and should be done first? Why?
 - If you had an extra \$5 to \$15, what would you have covered? Why?



FEMA



Activity – Report Out (10 Min)

Share your observations with the class:

- Which 2-3 activities are most important and should be done first? Why?
- If you had an extra \$5 to \$15, what would you have covered? Why?



FEMA



Cybersecurity Simulation Overview

The Organizations

There are six organizations in the simulation:

- City Government (Treasurer Office)
- City Utilities
- Community Bank
- Community Hospital
- K-12 School District
- Private Sector Business



FEMA



Simulation Overview

Community of Roadrunner Park

- Next: Four cyber events to test security plans
- Participant Goals:
 - Leverage a framework for cybersecurity planning.
 - Participate in an engaging view of community resilience.
 - Recognize the impact organizations have on the community.



FEMA

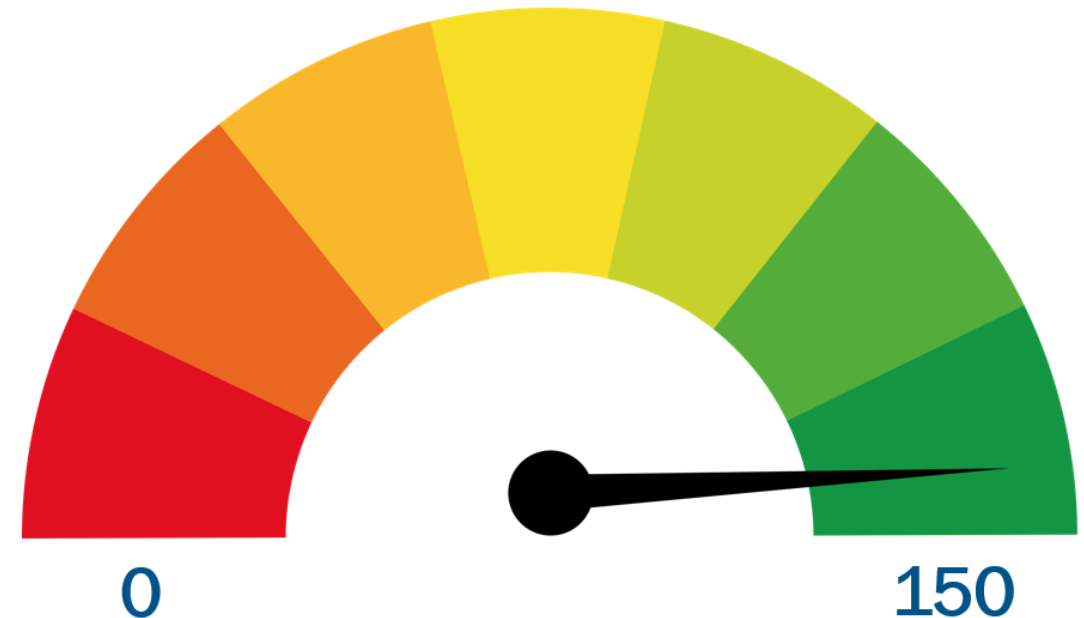


The Organization's Cyber Resilience Score

Initial *Cyber Resilience Score (CRS)* of **150** points.

- The CRS represents business continuity capability
- CRS score can change due to:
 - Organizational Impact
 - Community Impact

Cyber Resilience Score



FEMA

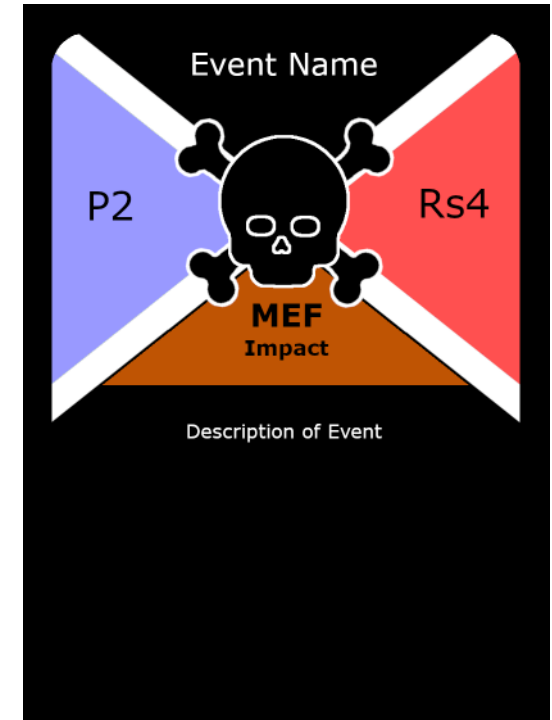
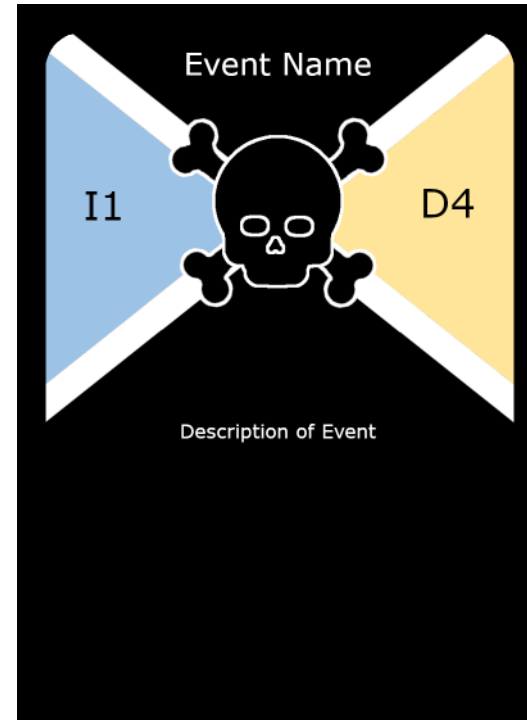


Simulation: Inject Phase

Identify the impact.

Characteristics of an Inject:

- Event Name
- Event Description
- Impacted Subcategories
- Potential: MEF Impact



FEMA



Simulation: Response and Recovery Phase

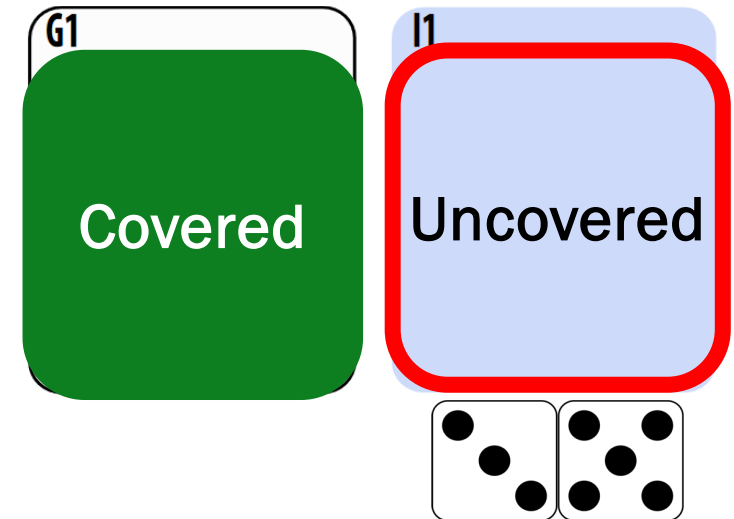
1. READ INJECT

- SLIDE – Reveals the inject
- READ – Review inject

2. DETERMINE IMPACT – For each impact:

- COVERED – Success
- UNCOVERED – Impacted
 - ROLL – Roll two die and add total
 - TOTAL – Represents CRS points lost

3. UPDATE SCORE – Add lost points to Score Sheet



CATEGORIES	EVENT 0
IMPACT 1	0
IMPACT 2	8



FEMA



Simulation: Scoring Phase

Scoring is updated on each Group's Score Sheet.

Scores can be impacted by:

- Successful cyber incidents
- Community-wide incident

SCORABLE CATEGORIES	SCORING RULES	EVENT 0 (PRACTICE)	EVENT 1	EVENT 2	EVENT 3	EVENT 4
IMPACT 1	Uncovered, roll 2 dice					
IMPACT 2	Uncovered, roll 2 dice					
ORGANIZATIONAL MEF	If <u>you</u> are impacted, lose points					
COMMUNITY MEF	If <u>anyone</u> is impacted, lose points					
END OF THE ROUND, EVENT SUBTOTAL	→					
ADJUSTMENTS						
ORGANIZATION'S CRS POINT TOTAL	150					



FEMA



Practice: Event 0 Activity (5 Min)

Roll the Dice

D1

Rs4

MEF
Secure Sensitive Information

Sunday morning, customers across the community begin reporting they are receiving emails from your organization demanding ransomware payments or their personally identifiable information will be posted on the internet. (All organizations lose an additional 10 CRS points this round.)

SCORABLE CATEGORIES	SCORING RULES	EVENT 0 (PRACTICE)
IMPACT 1	Uncovered, roll 2 dice	
IMPACT 2	Uncovered, roll 2 dice	
ORGANIZATIONAL MEF	If <u>you</u> are impacted, lose points	
COMMUNITY MEF	If <u>anyone</u> is impacted, lose points	
END OF THE ROUND, EVENT SUBTOTAL	→	
ORGANIZATION'S CRS POINT TOTAL	150	



FEMA



Remember . . .

- This is a simulation.
- There is an element of chance due to its gamification presentation.
- Don't fight the scenario.
- The intention of this activity is to facilitate discussion of cybersecurity topics and strategies in a fun way.



FEMA



Simulation Details



- This simulation:
 - Represents a city-wide cyber-attack.
 - The attack occurs over a one-week time frame.
- Planning Stage Complete:
 - All covered cybersecurity controls have been implemented in your organization.
 - Additional resources and budget for planning activities are **NOT** possible in between events.



FEMA



Event 1

Event 1: Inject Actions

In your organization's group:

- Review and discuss the Inject.
- For each impacted planning sub-category:
 - If the sub-category is covered, do nothing.
 - If the sub-category is NOT covered, roll two dice and deduct points equal to the sum of the dice from your Cyber Resilience Score.
- Your Reporter should be prepared to discuss the inject and the impact on your organization with the group.

1:00

2:00

3:00

4:00

5:00



FEMA



Event 1: Lost Assets

Monday morning, a key person in your office notifies the IT staff that their laptop has been stolen when they left their computer bag unattended.



FEMA

Planning Board IMPACT:

P3 Encryption

The card features a blue background with a yellow padlock icon in a circle at the top. Below the icon, the text reads "Encryption Protect 3". A white diagonal banner across the middle contains the text "Encryption Protect 3". Below the banner, a paragraph states: "The confidentiality, integrity, and availability of the organization's data at rest, in use, and in transit are protected." At the bottom left, there is a small white box with the text "\$5".

D4 Mobile Device Management

The card features a yellow background with a black smartphone icon at the top. Below the icon, the text reads "Mobile Device Management Detect 4". A white diagonal banner across the middle contains the text "Mobile Device Management Detect 4". Below the banner, a paragraph states: "The organization centrally manages the security of mobile devices through systems and policy." At the bottom left, there is a small white box with the text "\$5".



Community Events 1

Schools – An email promising a free vacation is sent to all personnel in the school district.

Hospital – Email sent to employees requiring them to click the link to install a software update. When clicked nothing happened.

Bank – The CEO reported a laptop stolen.

Utilities – The VOIP phone system stopped working

Local Businesses – Cyber attack identified. Software customer accounts have been compromised. The biggest customer are county governments.



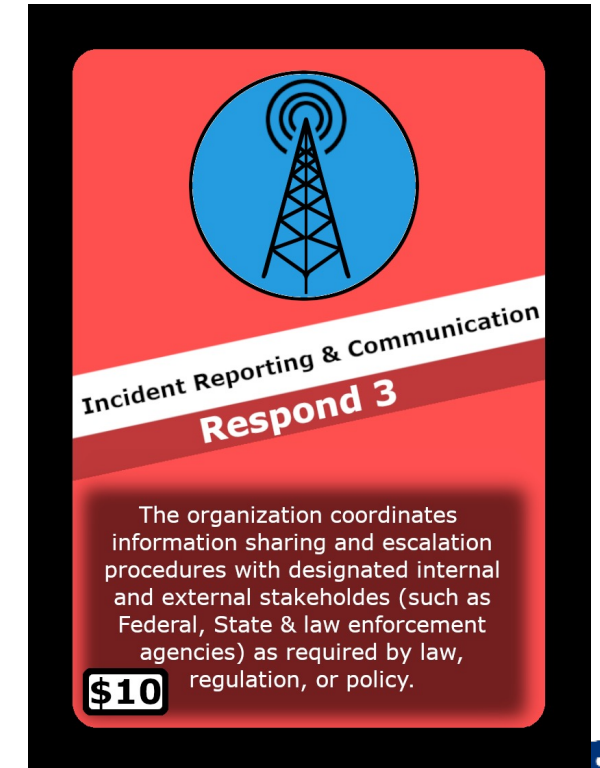
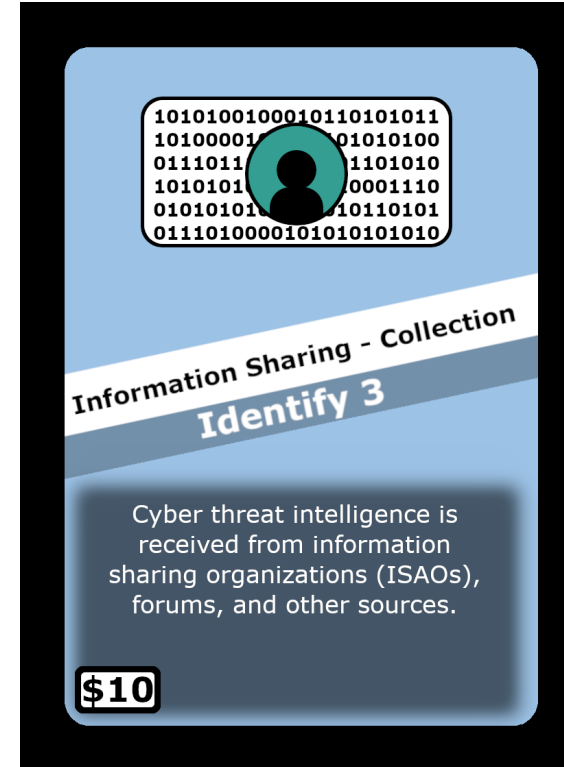
FEMA



Event 1: Information Sharing Trigger

- If you covered both:
 - Identify 3: Information Sharing – Collection
 - Respond 3: Incident Reporting & Communication
 - Receive one additional planning card.

Review your unused planning cards, select one and cover an uncovered spot on the board.



FEMA



Community Cybersecurity Information Sharing

- What is information sharing and why is it essential for community cybersecurity?
- Low-cost solutions can help organizations achieve more with less.
- Consider joining:
 - MS-ISAC, TxISAO, and ACTRA
 - InfraGard
 - AIS/HISN



FEMA



Event 2

Event 2: Backdoor

Monday morning, your office receives a phone call from your outsourced software firm that serves multiple county government offices.

You are notified that the firm has experienced a cyber incident and your office should shut down any computers using the software.

The firm has shut down its servers and vital data storage services will be down for several days.

MEF IMPACT



FEMA

Planning Board IMPACT:

G2 Risk management



I4 Supply chain management



Community Events 2

Schools – Flooded with phone calls from parents asking where to pick up their children because the school is closing due to a gas leak.

MEF COMPROMISE ALL ORGANIZATIONS LOSE 10 POINTS

Hospital – Breach from a phishing email. Forced to shut down many non-essential computers to contain malware. **MEF IMPACT**

Bank – The mortgage loan process is down. All loan processing is halted. **MEF IMPACT**

Utilities – Garbage pickup is delayed due to traffic signal malfunctions. The automated vehicle tracking system is down. Drivers report vehicles are malfunctioning and shutting down.

Businesses – The online credit card system is compromised. Customers are notified.
MEF IMPACT



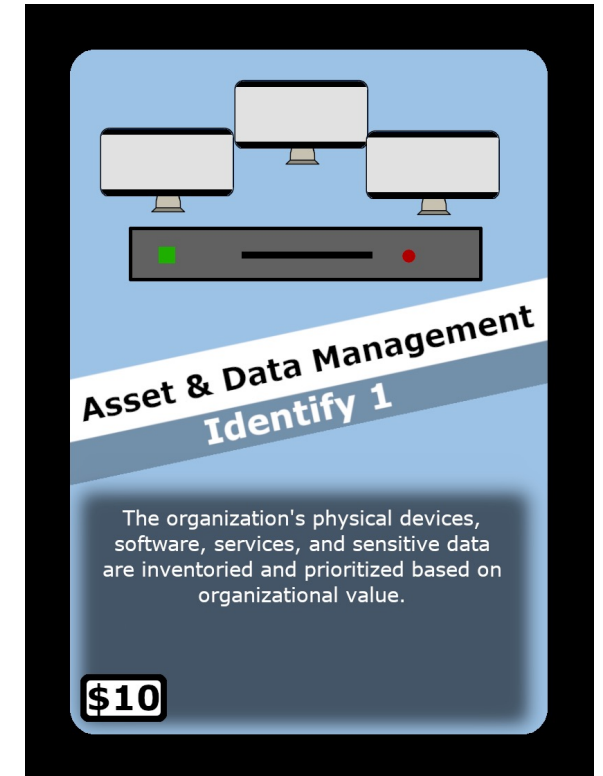
FEMA



Event 2: MEF and High Value Asset Trigger

- If you covered both:
 - Govern 1: Organizational Priorities
 - Identify 1: Asset & Data Management
 - Receive one additional planning card.

Review your unused planning cards; select one and cover an uncovered spot on the board.



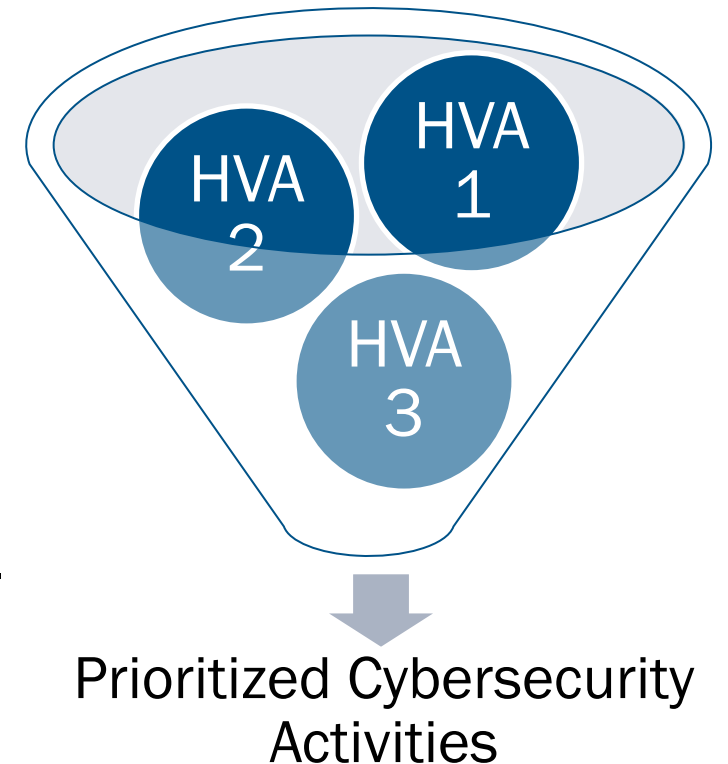
FEMA



Relationship Between Mission, Assets and Priorities

HVAs can be any information or information system that relates to one of the following categories:

- Informational value
 - Information or information system that processes, stores or transmits the information is of high value.
- Mission essential
 - The organization owning the information or information system cannot accomplish its mission essential functions (MEF) within expected timelines without the information or information system.
- Protective assets
 - The assets serving critical functions for maintaining security or resilience.



FEMA



Event 3

Event 3: Cash Only

Wednesday morning, several customers report they could not make online payments for county services.

Out of an abundance of caution, the county leaders decide to have the impacted servers taken off line.

Online payment services across the county government are suspended until the situation can be assessed.

MEF IMPACT affecting whole community. – 10 points



FEMA

Planning Board IMPACT:

P4 Backups



The confidentiality, integrity, and availability of the organization's data at rest, in use, and in transit are protected.

Rc2 System and data recovery



The organization centrally manages the security of mobile devices through systems and policy.



Community Events 3

Schools – Ransomware attack. The network is down. Teachers and administrators report they cannot access any data. **MEF IMPACT.**

Hospital – Environmental and mechanical industrial control systems are not working such as HVAC, elevators, and others.

Bank – Reports of ATMs malfunctioning (not working or dispersing random amounts of money). **MEF IMPACT.**

Utilities – The water SCADA system is down. Shutting off water to citizens and businesses. **MEF IMPACT affecting whole community. – 10 points**

Local Businesses – Reports of e-commerce customer accounts have been altered. **MEF IMPACT.**



FEMA



Event 3: Federal/State Assistance Special Action

You may be eligible for Federal/State assistance if you covered Respond 3: Incident Reporting & Communication.

- Federal/State assistance may be available, but resources are limited. Thus, only one organization may receive assistance.
- The assistance priority is: City Government, City Utilities, Community Hospital, K-12 School District, Community Bank and then Local Businesses.

Review your unused planning cards, select one, and cover an uncovered spot on the board.



FEMA

The card features a red background with a blue circle containing a black radio tower icon with signal waves. A white diagonal banner across the middle contains the text "Incident Reporting & Communication" and "Respond 3" in red. Below the banner, white text describes the organization's role in coordinating information sharing and escalation procedures. A black box in the bottom left corner contains the value "\$10".

Incident Reporting & Communication
Respond 3

The organization coordinates information sharing and escalation procedures with designated internal and external stakeholders (such as Federal, State & law enforcement agencies) as required by law, regulation, or policy.

\$10



Federal/State Assistance is Limited

- Post-attack federal assistance is limited:
 - Most federal assistance involves information sharing.
 - Fly-away and recovery teams are extremely limited.
 - In a significant attack, criminal and national security considerations may prevent disclosure.
- State-based assistance is highly contingent on the specific state and services they provide.

In both cases, advanced contact and planning are crucial to improving the chance of receiving assistance.



FEMA



Event 4

Event 4: Data Entry Dilma

Friday afternoon, your office receives multiple phone calls from different county offices. They are reporting that their accounts seem to reflect incorrect amounts of money.

When accounts are pulled up, all entry amounts say \$5.

MEF IMPACT affecting whole community. – 10 points

Planning Board IMPACT:

D3 Virus Protection



Rs3 Incident Reporting and communication



FEMA



Community Events 4

Schools – Janitorial service suffered a breach several months ago and are now required to notify customers.

Hospital – ER computers are not available. Staff report patient records have been altered or deleted. Hospital begins to reschedule surgeries and send patients to other facilities. **MEF IMPACT**

Bank – Customers report they are unable to make investment trades. **MEF IMPACT**

Utilities – Computers and pumping systems are down for water and wastewater. No Water in the community and sewage backs up. Several intersections around the county courthouse and other locations are flooded with sewage. **MEF IMPACT affecting whole community. – 10 points**

Local Businesses – Remote employee reports sluggish computer. IT personnel find updates have not been performed on the laptop.



FEMA



Event 4: Cyber Insurance

If you covered Recovery 4: Cyber Insurance, receive 25% of your lost points back. (Rounded up)

Points Lost	25%
2	1
6	2
10	3
14	4
18	5
22	6
26	7
30	8
34	9

Points Lost	25%
38	10
42	11
46	12
50	13
54	14
58	15
62	16
66	17
70	18

Points Lost	25%
74	19
78	20
82	21
86	22
90	23
94	24
98	25
102	26
106	27

Insurance
Cyber

Cyber Insurance
Recovery 4

The organization purchases Cyber Insurance coverage to protect itself from financial losses and liabilities due to cyber attacks or data breaches.

\$15



FEMA



Cyber Insurance

First Party

- Incident Management, Analysis & Containment
- System & Data Recovery
- Legal Services
- Public Relations, Notification & Call Center
- Business Interruption
- Cyber Extortion

Third Party

- Broad coverage for failure to protect data
- Vicarious liability coverage for vendors (Business Associates, Tech Providers (SaaS, PaaS, etc.))
- Regulatory fines & penalties
- Civil & Class Action Defense

Typical Exclusions

- Poor security processes
- Prior breaches
- Human Error
- Insider attacks
- Pre-existing vulnerabilities
- Technology system improvements
- Force Majeure



FEMA



Other Considerations – Physical Event Causing a Cyber Outage

EXTENDED INTERNET OUTAGE

A substation was shot at in the early morning. The attack required repairs that cost more than \$250,000 causing a power outage in your area.

As of April 2024, the average lead time for a substation transformer is 120 weeks, but can range from 80 to 210 weeks.

This is due to supply shortages and an inflexible market. In 2021, the lead time was around 50 weeks.



FEMA



Summary

Your Takeaways:

- Develop or Update your Continuity Plans.
- Know what your high value assets and organizational mission essential functions are. Communicate these with your IT Department.
- Experienced how mission essential function failure can have cascading effects throughout a community.
- Make connections to help.



FEMA



Thank You



Natalie Sjelin
Director of Training, CIAS
Natalie.Sjelin@utsa.edu
210-458-2119



FEMA



Panel Discussion Considerations

- Develop or Update your Continuity Plans. How often do you update plans?
- Know what your high value assets and organizational mission essential functions are. Communicate these with your IT Department.
- Experienced how mission essential function failure can have cascading effects throughout a community. Include community organizations that could impact your mission essential functions.
- Include how/when you will ask for State and Federal cyber incident response capabilities.
- Do you have or do you want cyber insurance?
- Consider creating a county treasurer working group for the State of Ohio for information sharing.



FEMA

