Crises Due to Unpredictable/Unavoidable Events

Carol Woody, PhD

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0494

Agenda

Introduction: Definitions & Responses

Learn from Crises Events

Risk Management: Evaluating the Unpredictable

Cybersecurity Risk

Preparing for a Cyber Attack: Cybersecurity Risk Management

Wrap-up

Introduction: Definitions & Responses

Unpredictable/Unavoidable Crises Events

What do we mean?

- **Unpredictable**– unforeseeable, uncertain, unsure, doubtful, dubious, iffy, dicey, up in the air, maybe, possibly
- **Unavoidable** – inevitable, assured, certain, predestined, predetermined, fated, unpreventable
- **Crises** – emergency, disaster, catastrophe, calamity, plight, predicament, mess, dire straights, difficulty, extremity, turning point, crossroads, watershed, moment of truth, zero hour, point of no return, doomsday

Examples?

Some Examples

Personal
- health (heart attack, stroke, car accident)
- financial (house robbery, house fire, car theft, identity theft)

Organization
- employee crises (strike, walk-out)
- compliance (OSHA, IRS)
- physical (fires, plane crash, oil spills)
- cyber (denial of service, data thefts)

Community/region
- weather (major hurricane damage, ice storms)
- utilities failures (power, water)
- pollution

Country
- war
- missile attack
- famine

How do we respond?

Response Options

Recognize and respond –react when the time comes

Prepare/resist

- *Transfer*—A risk is shifted to another party (insurance or outsourcing).
- *Avoid*—Activities are restructured to eliminate the possibility (move away from flooding areas and high crime areas)
- *Mitigate*—Actions are implemented in an attempt to reduce or contain crises (fire proofing, redundant systems)

Recover

Learn from Crises Events

Complex Failure: 2003 Power Blackout - 1

August 2003, 50 million electricity consumers in Canada and the northeastern U.S. lost power.

Multiple failures (handled independently) occurred over 4 hrs.

- Mid-day, 3 high-voltage lines went out of service, trees too close
- Race condition (software) disabled the alarm system that notified operators of line problems.
  - hot backup failed—hardware redundancy only
  - alarm system restart required full-control system reboot (four integrated subsystems requiring > 30 min)
  - IT chose to wait to off-peak hours to reset the system
- Alarm monitors did not know their system failed; not notified by IT
  - assumed all was well—no alarms
  - did not notice their system power failure—automatic power backup

Complex Failure: 2003 Power Blackout - 2

Independent power grid monitoring at different site also failed.

System monitoring and modeling application samples the current state and projects future system state.

Warnings are raised when projected state differs significantly from realized state.

- Data errors resulted from the downed lines; IT had to correct errors manually.
- After fixing the data (60 minutes), the IT person forgot to restart the monitor before leaving for lunch.
- Restart failed after lunch as data was out of synch with live system.
- Monitor finally restarted about 30 minutes before final failure (insufficient time to analyze discrepancies and respond).

2003 Power Blackout Observations

- Technical failures required too lengthy a recovery time and systems were allowed to continue running in degraded mode
  - No one understood the impact of this mode of operation
  - No procedures were in place to handle this non-standard option
- Hardware redundancy will not accommodate software failures.
- Critical mission dependencies were not recognized.
  - lack of operational ability to identify early warning signs of failure
  - independent monitoring not operationally robust
- No one understood the implications of the decisions they made

Hurricane Katrina, New Orleans 2006 (category 5) - 1

Planning for hurricane resources and response used a standard hurricane as the baseline (category 3)

- Exercises were conducted for a standard event
- Local boards were not aware that the “standard” was insufficient

Levees were known to be critical and responsibility was assigned to a local levee board in each precinct

- No warning systems in place to monitor levee stresses
- No coordination among the various local boards
- Levee strength as designed by the US Army Corp of Engineers for a standard hurricane (moderate category 3)

No “mandatory evacuation” was declared because this required officials to confirm compliance (costly) – instead “recommended”, “suggested”, “highly suggested” were announced

Hurricane Katrina, New Orleans 2006 (category 5) - 2

Standards are useful but not sufficient

- Lack of understanding of the meaning of “standard” further reduces their value

Exercises are useful but not sufficient

- Lack of understanding of how an exercise differs from reality further reduces its value

Local control of a shared resource is useful but not sufficient – the levees broke at the boundaries which were largely unmaintained (no one had responsibility for the meeting points)

Communication is critical but the recipient must have a level of understanding of the conditions being described and the actions to be taken

Risk Management:
Evaluating the Unpredictable

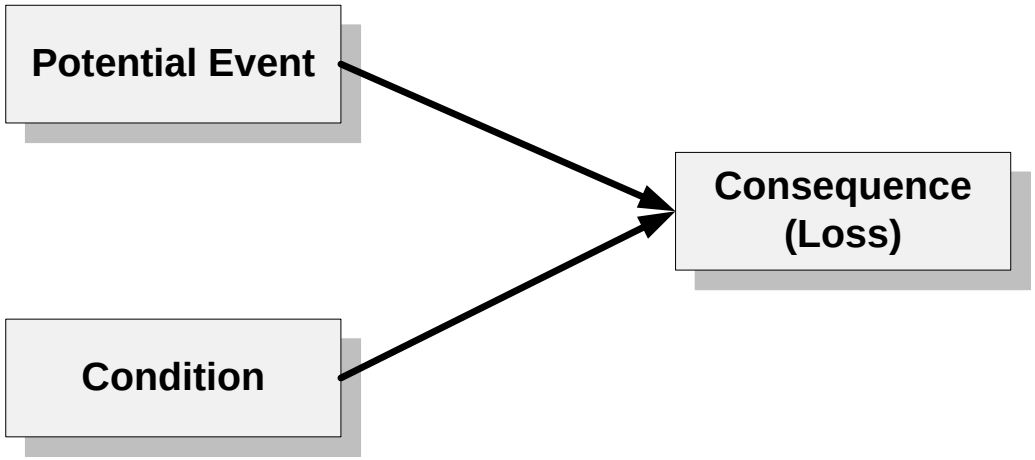
What Is Risk?

The probability of suffering harm or loss (or gain in some contexts)

A measure of the likelihood that an event will lead to a loss coupled with the magnitude of the loss

Risk requires the following conditions:[1]

- A potential loss
- Likelihood
- Choice



1. Charette, Robert N. *Application Strategies for Risk Analysis*. New York, NY: McGraw-Hill Book Company, 1990.

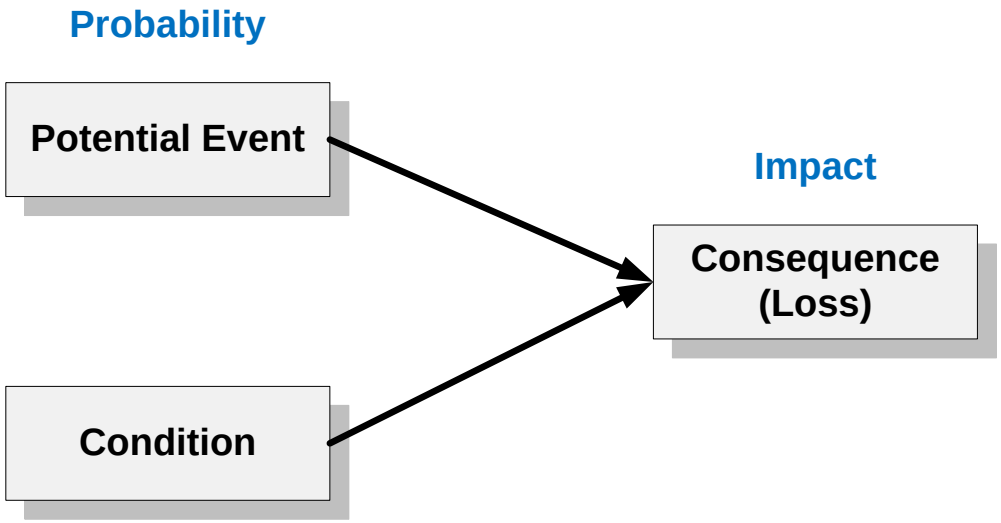
Risk Measures

Probability

- The likelihood that an event will occur

Impact

- The loss that occurs when a risk is realized



Risk exposure

- The magnitude of a risk based on current values of probability and impact

Types of Risk Control Actions

Recognize and respond

- Monitor the event and take action when it is detected.

Resist

- Implement protection measures to reduce exposure to the event or minimize any consequences that might occur.

Recover

- Return to an acceptable state if the consequences or losses are realized.

Cybersecurity Risk

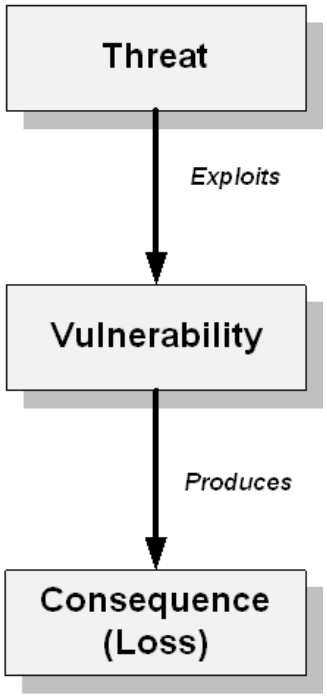
Three Components of Cybersecurity Risk

Threat *(Potential Event)*

- A cyber-based act, occurrence, or event that exploits one or more vulnerabilities and leads to an adverse consequence or loss

Vulnerability *(Condition)*

- A weakness in an information system, system security procedures, internal controls or implementation that a threat could exploit to produce an adverse consequence or loss; a current condition that leads to or enables security risk



Consequence

- The loss that results when a threat exploits one or more vulnerabilities; the loss is measured in relation to the status quo (i.e., current state)

What is Known about the Vulnerability

National Vulnerability Database (NVD) (nvd.nist.gov)

- Total vulnerabilities registered: 104,893
- New this year: 4,519

Common Weaknesses Established (cwe.mitre.org)

- 716 software weaknesses
- Top 25 (unchanged since 2011) include buffer overflow, cross-site scripting, memory/data leaks

Why should we care?

Everyone is now in the Software Business

The report *Critical Code: Software Producibility for Defense*, issued in 2010, states that “software has become essential to all aspects of military system capabilities and operations.”

- 1960: Software handled 8% of the F-4 Phantom fighter’s functionality.
- 1982: Software handled 45% of the F-16 Fighting Falcon’s functionality.
- 2000: Software handled 80% of the F-22 Raptor’s functionality.

Software is Addressing More Functionality

All software has defects.

Software quality determines the defect volume and 1-5% are vulnerabilities

Software volume is increasing

- F-22 fighter aircraft (2005)
  - 1.7 MLOC
- F-35 Lightning II fighter aircraft (2016)
  - 24 MLOC

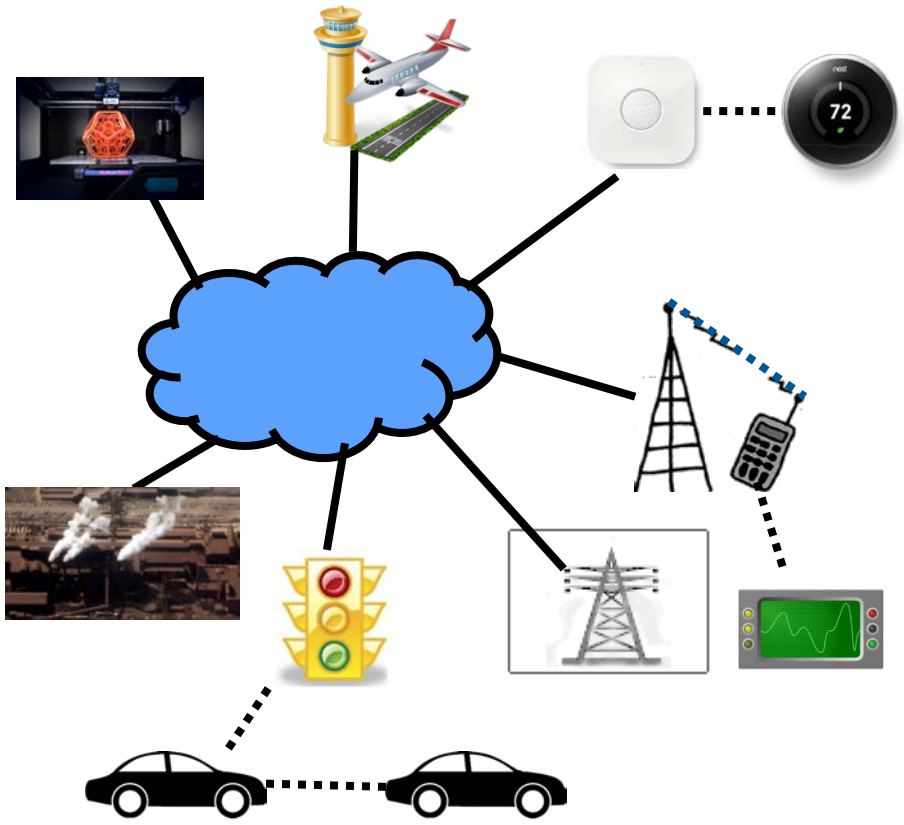
Likelihood of software vulnerabilities is increasing as software volume increases

Defects per million lines of code (MLOC)
Best-in-class code:
<600 defects per MLOC
Very good code:
600 to 1,000 defects per MLOC
Average quality code:
6000 defects per MLOC

Capers Jones, sqgne.org/presentations/2011-12/Jones-Sep-2011.pdf

1-5 % of defects are vulnerabilities.
Woody, Carol; Ellison, Robert; and Nichols, William. Predicting Software Assurance Using Quality and Reliability Measures. CMU/SEI-2014-TN-026. Software Engineering Institute, Carnegie Mellon University. 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=428589)

More Software Links Other Systems



- Cellular
  - Main processor
  - Graphics processor
  - Base band processor (SDR)
  - Secure element (SIM)
- Automotive
  - Autonomous vehicles
  - Vehicle to infrastructure (V2I)
  - Vehicle to vehicle (V2V)
- Industrial and home automation
  - 3D printing (additive manufacturing)
  - Autonomous robots
  - Interconnected SCADA
- Aviation
  - Next Gen air traffic control
  - Fly by wire
- Smart grid
  - Smart electric meters
  - Smart metering infrastructure
- Embedded medical devices

Opportunities for Security Attacks are Increasing

Weaknesses exist that an attacker can exploit

Required three elements:

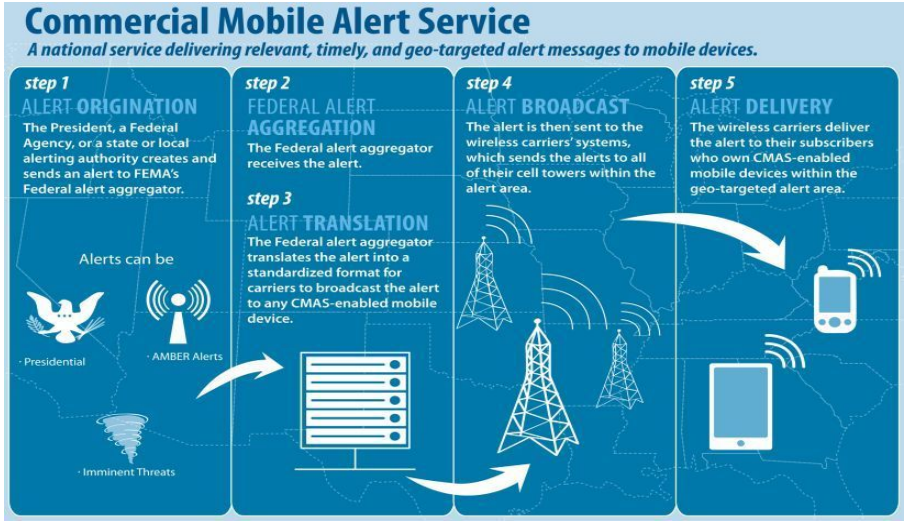
- a system susceptibility or flaw *(condition)*
  - Millions of lines of software code handling an ever increasing amount of functionality
  - Thousands of software vulnerabilities
  - Increased reliance on commercial and open source software
- attacker access to the flaw, and
  - Increased connectivity linking systems to other systems and connecting to new types of devices (Internet of Things)
  - Increased system and device remote communication capability
- Attacker capability to exploit the flaw *(potential event)*
  - Access to the same tools and techniques used to build software
  - Reverse engineering capabilities for commercial and open source
  - Malware and attack platforms and frameworks

Preparing for a Cyber Attack: Cybersecurity Risk Management

SERA Task 1: *Wireless Emergency Alerts (WEA)*

WEA is a major component of the Federal Emergency Management Agency (FEMA) Integrated Public Alert and Warning System (IPAWS).

- Enables federal, state, territorial, tribal, and local government officials to send targeted text alerts to the public via commercial mobile service providers (CMSPs).
- Customers of participating wireless carriers with WEA-capable mobile devices will automatically receive alerts in the event of an emergency if they are located in or travel to the affected geographic area.

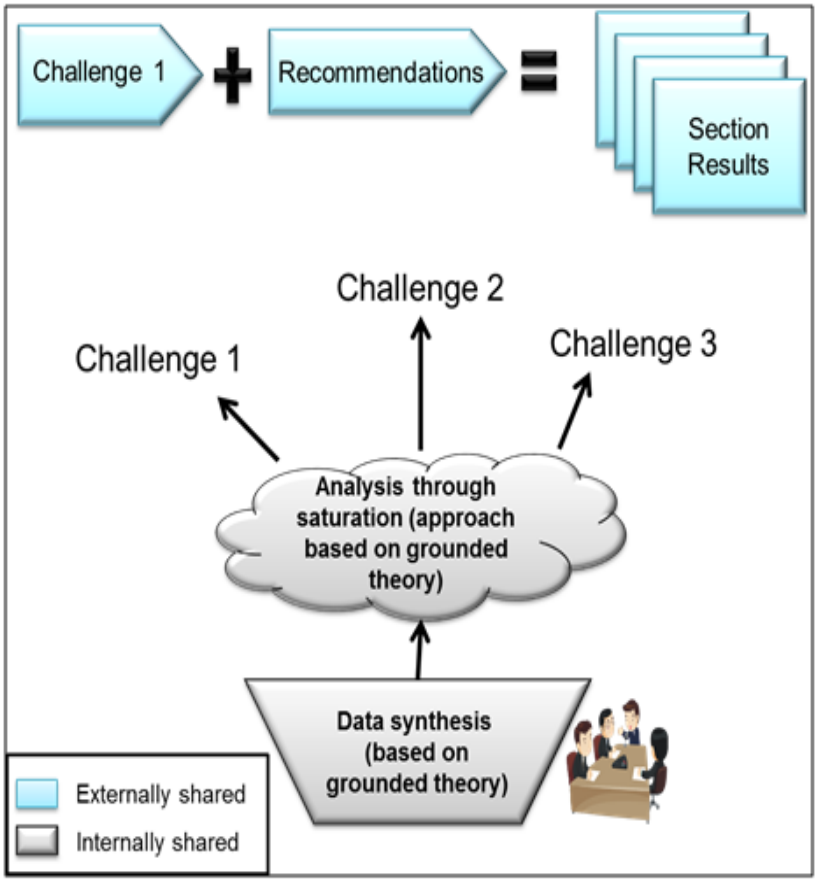


AO Data Collection and Research Approach

Structured Interview-based Research Approach and Mission Thread Workshop (MTW) Method

Interviews conducted with:

- 28 Emergency Management stakeholders
  - e.g., Adams County 911, Colorado, California Emergency Management Agency, NCMEC, NOAA
- 14 Vendors
  - e.g., Everbridge, Alerting solution, DAS
- 6 Expert or Academic Resources
  - e.g., Gary Hamm, Art Botterell



WEA Security Pocket Guide

1. Has your organization considered cybersecurity risks?
2. How would a cyber attack affect your operations?
3. Do you know how an attacker might access your system?
4. Have you determined which areas of your system present the greatest security risks?
5. Are there ways that your systems are used, configured, or accessed that could be a security risk?
6. Do you know how to reduce those risks?
7. Is there a systematic way to identify and mitigate security risks?

AO Security Findings

Analysis of security questions for alert originator interviews:

- Stakeholders most commonly discussed access control, and within access control, their responses typically related to password-based control.
- Though alerting technology is evolving, stakeholders' security knowledge is not keeping pace.
- Security is a multifaceted area and the stakeholders lack an understanding of the issues.

Analysis of security questions for alerting system vendors:

- Vendors were concerned with a greater variety of security issues than were the alert originators.
- Vendors seemed to be more aware of current security concepts.
- Vendors seemed to be more aware of the security guidelines in the IPAWS-OPEN MOA than their alert originator counterparts.

Alert Originators *do not have a security mindset* at the leadership/management level.
Security is seen as "someone else's job."

Class Discussion - 1

You are a senior manager at a multi-national corporation with offices in Hawaii. You receive a call from your onsite manager who just received an emergency alert that a missile is headed your way. What should they do?

Are you prepared?

How do you respond?

How will you recover?

Security Engineering Risk Analysis (SERA)

What

- A systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain

Why

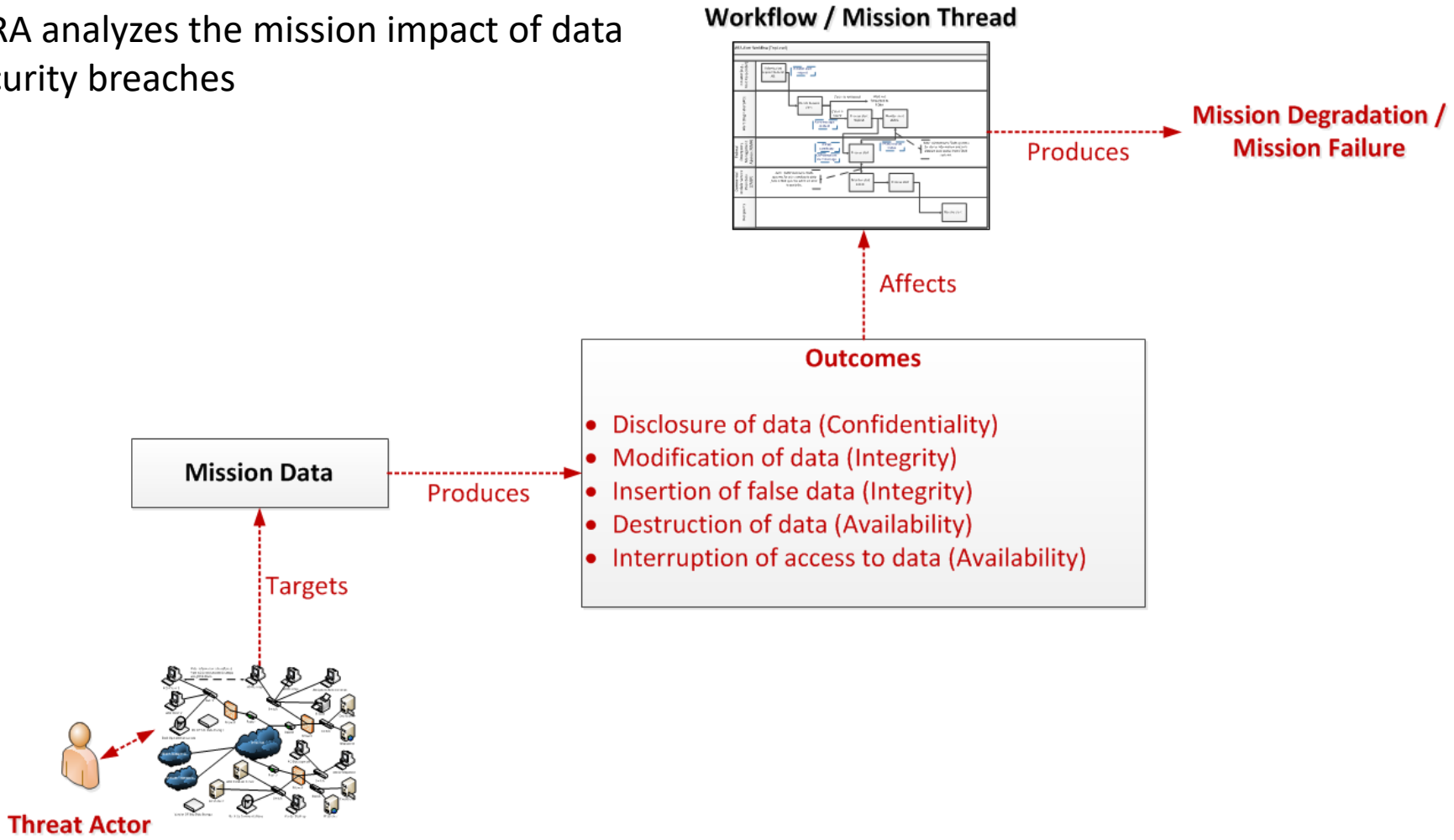
- Build security into software-reliant systems by addressing design weaknesses as early as possible (e.g., requirements, architecture, design)
- Assemble a shared organizational view (business and technical) of cybersecurity risk

Benefits

- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems

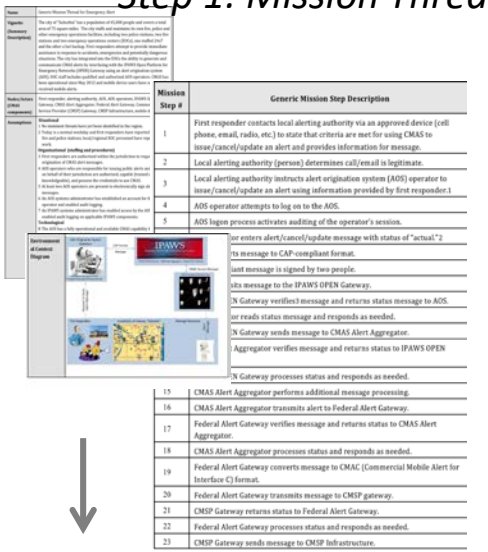
SERA Approach: *Focus on Mission Impact*

SERA analyzes the mission impact of data security breaches



Cybersecurity Strategy Approach

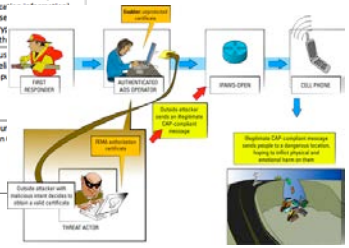
Step 1: Mission Threads



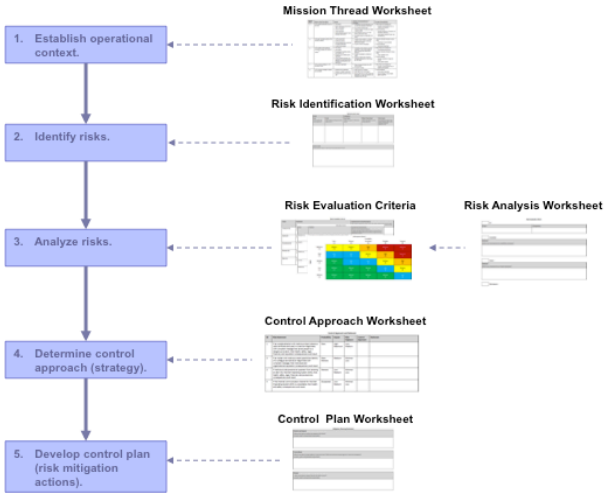
Mission Step #	Generic Mission Step Description
1	First responder contacts local alerting authority via an approved device (cell phone, email, radio, etc.) to state that criteria are met for using CMAS to issue/cancel/update an alert and provides information for message.
2	Local alerting authority (person) determines call/email is legitimate.
3	Local alerting authority instructs alert origination system (AOS) operator to issue/cancel/update an alert using information provided by first responder.1
4	AOS operator attempts to log on to the AOS.
5	AOS logon process activates auditing of the operator's session.
	or enters alert/cancel/update message with status of "actual."2
	ts message to CAP-compliant format.
	ust message is signed by two people.
	sits message to the IPAWS OPEN Gateway.
	N Gateway verifies3 message and returns status message to AOS.
	or reads status message and responds as needed.
	N Gateway sends message to CMAS Alert Aggregator.
	Aggregator verifies message and returns status to IPAWS OPEN
	N Gateway processes status and responds as needed.
15	CMAS Alert Aggregator performs additional message processing.
16	CMAS Alert Aggregator transmits alert to Federal Alert Gateway.
17	Federal Alert Gateway verifies message and returns status to CMAS Alert Aggregator.
18	CMAS Alert Aggregator processes status and responds as needed.
19	Federal Alert Gateway converts message to CMAC [Commercial Mobile Alert for Interface C) format.
20	Federal Alert Gateway transmits message to CMSP gateway.
21	CMSP Gateway returns status to Federal Alert Gateway.
22	Federal Alert Gateway processes status and responds as needed.
23	CMSP Gateway sends message to CMSP Infrastructure.

Step 2: Threat & Vulnerability Assessment

Mission Step #	Mission Step Description	Assets	STRIDE Threat Identification[12] Examples	Example Vulnerabilities
1	First responder contacts local alerting authority via an approved device (cell phone, email, radio, etc.) to state that criteria are met for using CMAS to issue/cancel/update an alert, and provides information for alert message.	– Two people – Communication devices – Procedures/criteria	S: Fake first responder T: Data altered in transit I: Disclosure of authentication information D: Communications devices not operational	– Insecure Interaction Between Components – Porous Defenses o Missing encryption of sensitive data (authen- o Use ctyp rith
2	Local alerting authority (person) determines cell/email is legitimate.	– One person – Authentication info	S: Connect to the wrong person T: Tampering with info used to authenticate first responder E: Insider threat / man in the middle	– Porous o Rel inp
3	Local alerting authority instructs alert origination system (AOS) operator to issue/cancel/update an alert using information provided by first responder.	– Two people – Communication devices – Procedures/criteria	S: Fake alerting authority or AOS operator T: Tampering with data provided D: Communications are down	– Insecu tween



Step 3: Cybersecurity Risk Analysis



Step 4: Risk Mitigation Actions

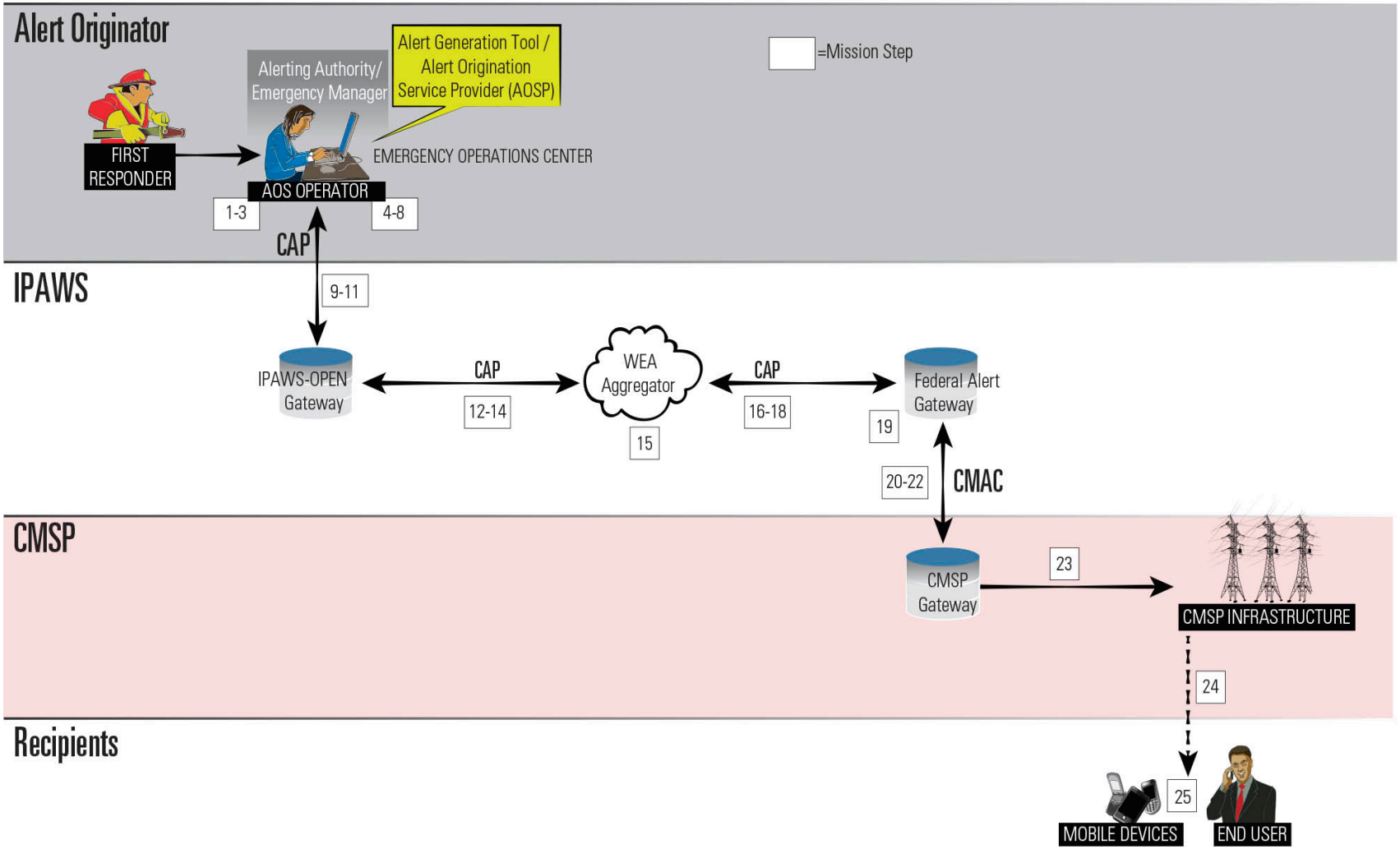
ALERT ORIGINATOR ROLE	CYBERSECURITY RISK MITIGATION ACTIONS	
	Adoption *Acquisition, Development, and Rollout*	Operations & Sustainment
Executive Manager	Champion and oversee application of CSRM activities in adoption.	Champion and oversee application of CSRM activities in operations and sustainment.
	Establish and enforce IT/IS governance practi	
Technology Acquisition Staff	Understand and articulate cybersecurity requirements and evaluation criteria to address products, services, and development and sustainment practices)	Elicit security conside operations and sustai these are incorporate requirements and evi
	Work with operations manager, operator/user, IT and IS man and security staff to fully understand, express, validate, and v	
Solution Provider (Technology Development) Staff		
Solution Provider (Service Provider) Staff		
Operations Manager		
Operator / User		
Information Technology (IT) and Information Security (IS) Managers		
System Administrators and IT/IS Incident Response Staff		

CSRM Plan Draft Outline

- Introduction
- Purpose
- Scope
- Audience
- Structure of Plan
- **Building and Using the CSRM Plan**
  - Identify Authors, Owners, and Users
  - Define Roles and Responsibilities
  - Provide Overview of How the Plan Was Constructed
- **CSRM Plan Activities**
  - Develop the CSRM Plan
    - Frame the Risk Context (described in our Chapter 3)
      - Prepare for CMAS Cybersecurity Analysis
    - Identify Threats and Vulnerabilities (described in our Chapter 4)
      - Conduct CMAS Cybersecurity Analysis
    - Assess and Prioritize Cybersecurity Risks (described in our Chapter 5)
    - Define Risk Mitigation Actions (described in our Chapter 5)
    - Allocate Risk Mitigation Actions to Roles (described in our Ch. 6)
      - People/Policy (policy, training, access)
      - Process (operational, assessment, mitigation, monitoring, disposal, etc...)
      - Technology (network, platform, application)
      - CMAS-Unique Elements
      - Cybersecurity threat, vulnerability, and risk assessment
      - Acquisition/Development cybersecurity risk mitigation
      - Operational cybersecurity risk mitigation
      - Cybersecurity risk management evaluation
      - Cybersecurity training
  - Implement the CSRM Plan (described in our Ch. 7)
  - Evaluate Effectiveness of the CSRM Plan (described in our Ch. 7)
  - Sustain the CSRM Plan (described in our Ch. 7)
    - Review Effectiveness
      - Periodically
      - After CMAS alerting events
      - After cybersecurity Incidents
      - In the face of technology upgrades/updates
  - Implement Improvements (described in our Ch. 7)
- **Appendix A: Cybersecurity Reference Standards and Guidance**

Planning and Governance: Develop, Train, Implement, Evaluate, and Improve CSRM Plan

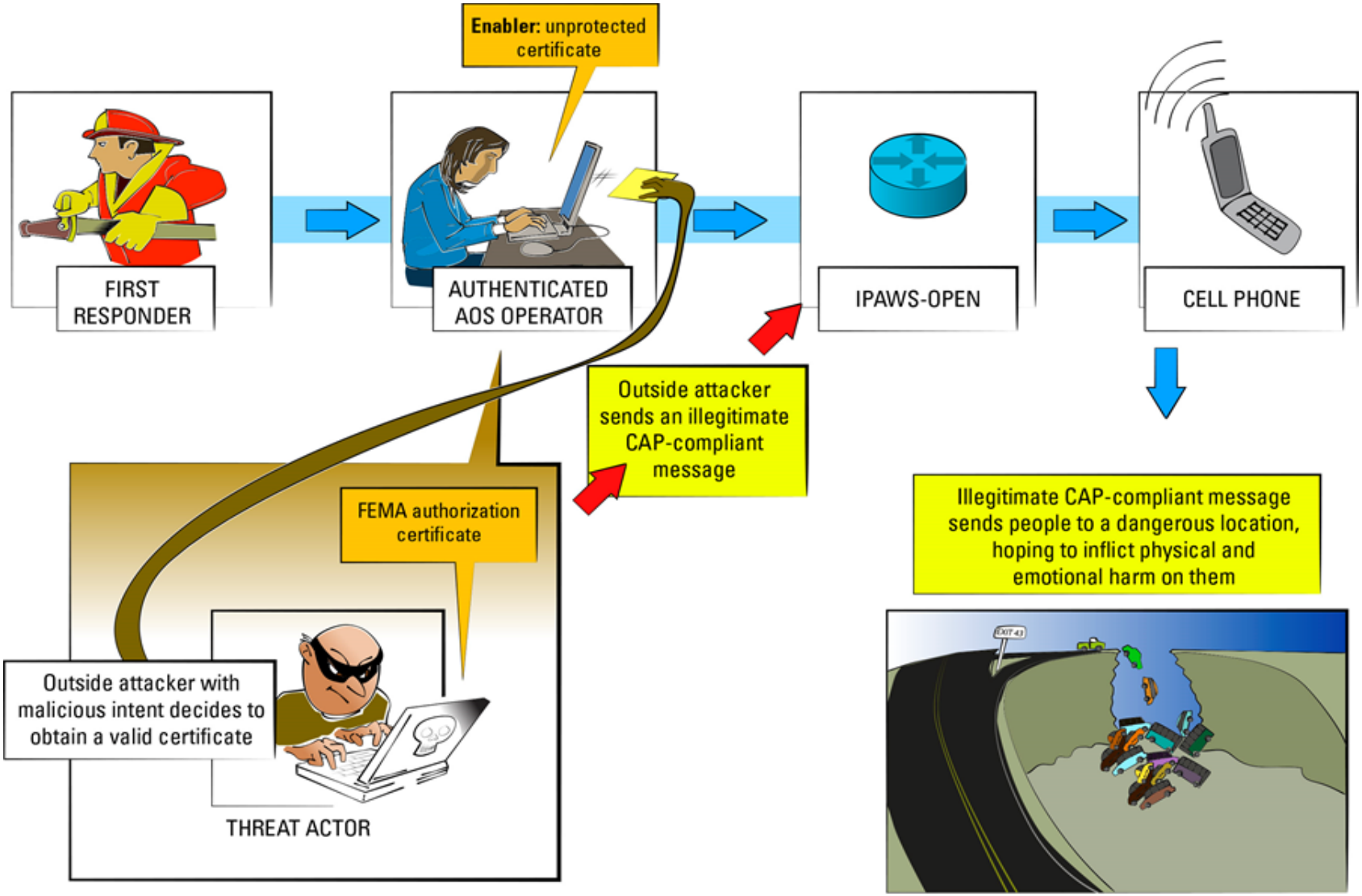
Step 1: WEA Mission Thread



Step 2: Example: *Risk Statement*

If an outside attacker with malicious intent obtains a valid certificate and uses it to send an illegitimate CAP-compliant message that sends people to a dangerous location, then health, safety, legal, financial, and reputation consequences could result.

Step 2: Example: *Risk Scenario*



Step 3: *Cybersecurity Risk Analysis*

What is the probability that the risk will occur? *Rational?*

What is the impact should that the risk occur? *Rational?*

Based on the estimated values of probability and impact, what is the resulting risk exposure?

Value	Definition	Context/Guidelines/Examples
Frequent (5)	The scenario occurs on numerous occasions or in quick succession. It tends to occur quite often or at close intervals.	≥ one time per month (≥ 12 / year)
Likely (4)	The scenario occurs on multiple occasions. It tends to occur reasonably often, but not in quick succession or at close intervals.	
Occasional (3)	The scenario occurs from time to time. It tends to occur "once in a while."	~ one time per 6 months (~ 2 / year)
Remote (2)	The scenario can occur, but it is not likely to occur. It has "an outside chance" of occurring.	
Rare (1)	The scenario infrequently occurs and is considered to be uncommon or unusual. It is not frequently experienced.	≤ one time every 3 years (≤ .33 / year)

Risk Exposure Matrix

Impact \ Probability	Rare (1)	Remote (2)	Occasional (3)	Probable (4)	Frequent (5)
Maximum (5)	Medium (3)	Medium (3)	High (4)	Maximum (5)	Maximum (5)
High (4)	Low (2)	Low (2)	Medium (3)	High (4)	Maximum (5)
Medium (3)	Minimal (1)	Low (2)	Low (2)	Medium (3)	High (4)
Low (2)	Minimal (1)	Minimal (1)	Minimal (1)	Low (2)	Medium (3)
Minimal (1)	Minimal (1)	Minimal (1)	Minimal (1)	Minimal (1)	Low (2)

Step 4: Determine Control Approach

A strategy for controlling each risk is determined based on

- Predefined criteria
- Current constraints (e.g., resources and funding available for control activities)

Control approaches for security risks include:

- *Accept*—If a risk occurs, its consequences will be tolerated.
- *Transfer*—A risk is shifted to another party (e.g., through insurance or outsourcing).
- *Avoid*—Activities are restructured to eliminate the possibility of a risk occurring.
- *Mitigate*—Actions are implemented in an attempt to reduce or contain a risk.

Sub-tasks:

- Prioritize risks.
- Select control approach.

Class Discussion - 2

You receive a call from the FBI that there is reasonable concern that your company's computer systems have been compromised. They have discovered evidence of data from your company on a hacker website and want to conduct an onsite evaluation.

Are you prepared?

How do you respond?

How will you recover?

Wrap-up

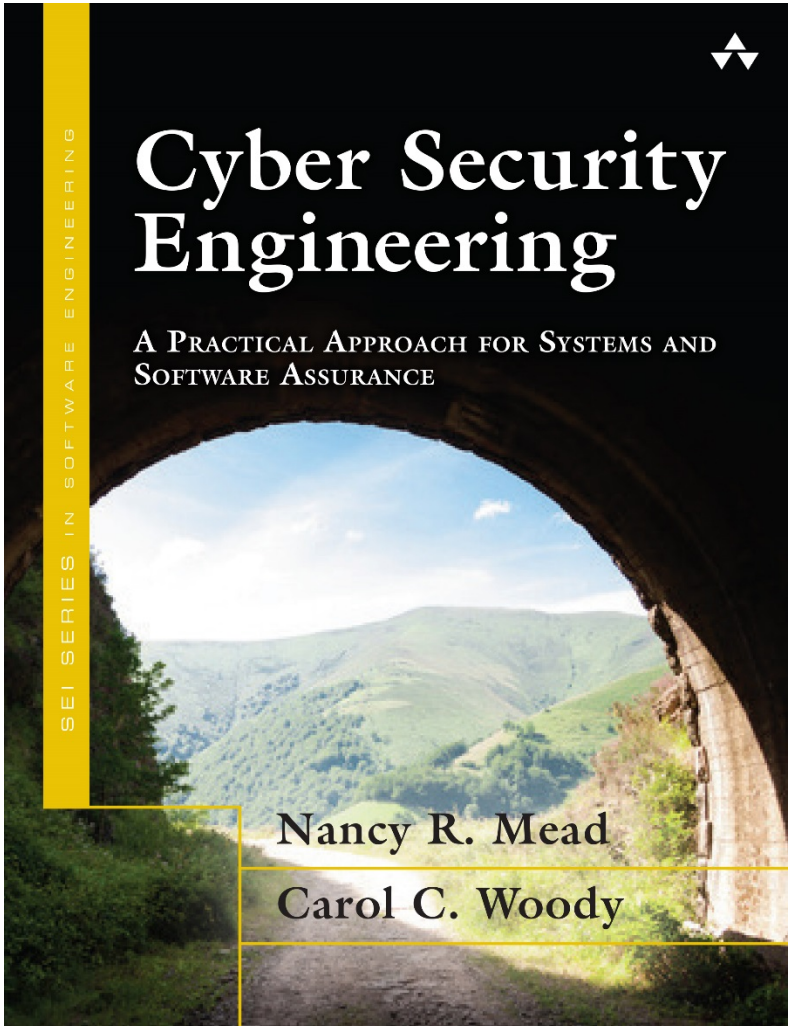
SERA: More Information

Alberts, C.; Woody, C.; & Dorofee, A. *Evaluating Security Risks using Mission Threads* (CMU/SEI-2014-TN-025). Software Engineering Institute, Carnegie Mellon University, 2014. http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_427329.pdf

Woody, C.; & Alberts, C. “Evaluating Security Risks using Mission Threads.” *CrossTalk 10,* 2 (September/October 2014): 14-19. http://www.crosstalkonline.org/storage/issue-archives/2014/201409/201409-Woody.pdf

Alberts, C.; Woody, C.; & Dorofee, Wireless Emergency Alerts Commercial Mobile Service Provider (CMSP) Security Guidelines, http://www.firstresponder.gov/TechnologyDocuments/Wireless%20Emergency%20Alerts%20CMSP%20Cybersecurity%20Guidelines.pdf

To Learn More on this Topic



Released November 2016 as part of the SEI Book Series and available for purchase on Amazon (paperback & Kindle versions)

For more information see https://insights.sei.cmu.edu/sei_blog/2016/10/seven-principles-for-software-assurance.html

Questions