Building a Risk Management Mindset

Sharon Mudd, PhD

13 November 2024

28th CISSE Colloquium, Tampa, FL

BUILDING A RISK MANAGEMENT MINDSET

agenda

- Speaker Intro
- Risk Primer
- The Problem
- Sample Curriculum

A LITTLE ABOUT ME

Sharon Mudd, PhD
Sr. Cybersecurity Researcher
Software Engineering Institute
@Carnegie Mellon University

MSIA

PhD

Organizer of Chaos

Builder of Cybersecurity Capabilities and Risk Management Culture

Architect of Information Security Governance and Risk Management Programs

Roles & Sectors

Software Developer
- Healthcare, Benefits

System Administration / Project Management
- Healthcare, State Gov

Security Administration / Management
- State Gov, Financial Software/Data Center

GRC / Information Risk Management
- Global Financial Services, State Gov, Global Retail, Global Education Services

Internal Audit
- Financial Services, State Services, Telecom, Security Services

Consulting & Concierge CISO
- Financial Services, State Services, Security Services

Professor / Mentor
- Information Security and Risk Topics and Careers

Career Highlights

Developed first GRC program for 3 international companies

Built Information Risk & 3rd Party Risk programs for 3 companies

FAIR Champion award 2019

BAPTIST HEALTH

RISK PRIMER

WHY IS UNDERSTANDING RISK IMPORTANT?

- Knowing what and where your risks are helps you decide where to spend your time and money.
- A successful information security strategy relies on understanding your risk posture.
- Without that, critical decisions are made with gut feelings, best guesses, or other uninformed factors.

If you don't understand risk:

You could miss the mark completely!

RISK PRIMER

Risk is the *likelihood* that a *threat* will successfully exploit a *vulnerability* to harm an *asset*.

Risk Equation:

All three must exist for there to be a risk.

THINKING ABOUT RISK #1

This is your car

- It is parked in front of your house.
- Car thefts in your neighborhood are at an all time high.
- There has been a lot of vandalism over the past month.

Is there a risk here?

- How much should you spend on car insurance?
- What about other protections?

THINKING ABOUT RISK #2

This is your car

- It is parked in front of your house.
- Car thefts in your neighborhood are at an all time high.
- There has been a lot of vandalism over the past month.

How does your risk evaluation change?

- How much should you spend on car insurance?
- What other protections could you use?

LITTLE BIT TOUGHER EXAMPLE

- You have a database that has already experienced failures twice this year.
- There is no redundancy and you haven't done a backup in a year.
- It hasn't been patched in 4 years and there are countless attacks 'in the wild' that could result in the theft or loss of your data.

Is there a risk here?

How much money should you spend to address this?

DETERMINING RISK LEVEL

What's the *impact* to **YOUR COMPANY** if bad things happen?

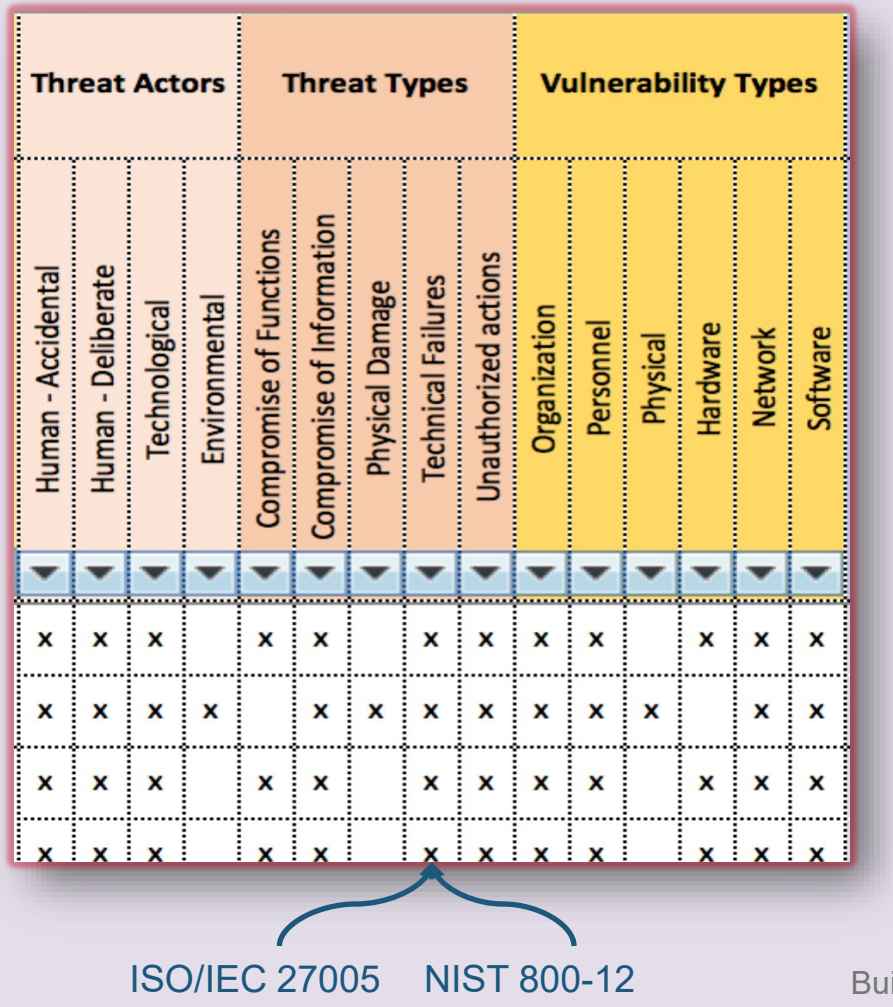
- What type of information does the asset contain?
- How much of that type of information?
- Where is that information located (region of the world)

What is the *likelihood* that a bad thing will happen?

- Is there an existing, viable threat?
- Is the asset vulnerable to that threat?

THREATS, VULNERABILITIES, IMPACTS

Classification



Assets	Threat Actor	Threat Type	Vulnerability Type	Impact
• Customer PII Data Store • Email	Human-Accidental	Emailed customer info to wrong client	Personnel	• Minimal (for 1-100 records) • Critical for >10,000 records
Customer PII Data Store	Technological	Technical Failure	Software (system crashed)	• Minimal (if good backup) • High (if no backup)
Primary Online Store Website	Human-Deliberate	Compromise of Functions / Unauthorized Actions (Hacked)	Network / Software	• High (if prices changed) • Critical (if taken offline)
Internal User Network	Human Deliberate	Compromise of Functions (Ransomware Attack)	Personnel / Network	• Medium (if isolated to user systems) • Critical (if primary datastore)

IMPACTS –OR- CONSEQUENCES

A FEW EXAMPLES

- VALUES, ETHICS, REPUTATION
- FINANCIAL
- BUSINESS CONTINUITY
- QUALITY
- COMPLIANCE
- DATA PRIVACY
- STUDENT/STAKEHOLDER EXPERIENCE

PRIORTIZING CORRECTIVE ACTIONS

Information / Cyber Security is not black and white. Choices have to be made according to the organizations risk appetite or tolerance posture.

THE PROBLEM

RISK MANAGEMENT SITS AT A CROSSROADS

Carnegie Mellon University

Interdisciplinary Bachelor of Computer Science and Arts (BCSA)

School of Computer Science concentration

- Programming, Data Structures, Algorithms
- Human AI Interaction, Designing Human Centered Software, Human Language for AI, AI Representation and Problem Solving
- Machine Learning
- Data Science
- Robotics
- Software Engineering, Web App Development, Computer Game Programming

Bachelor of Humanities and Arts (BHA)

Policy & Management Concentration

- Management Core (3 courses)
  - Decision making in complex or uncertain environments
  - Choices with mutually conflicting objectives

Cybersecurity & International Conflict

- National level view – landscape of cyber capabilities
  - Implications for State-sponsored malicious actors
  - Balancing offensive and defensive cybersecurity
  - Military-focused cyber operations

RISK MANAGEMENT SITS AT A CROSSROADS

GEORGETOWN UNIVERSITY
School of Continuing Studies

online

Master of Professional Studies

Cybersecurity Risk Management

- Defense revolves around people to bridge gaps between security policies, information technologies, and human behaviors

Indiana University

online

Master of Science

Cybersecurity Risk Management

- Next generation of cybersecurity professionals
- Cross-disciplinary approach between schools of Technology, Business, and Law

online

PennState World Campus

Bachelor of Science

Security and Risk Analysis

- Identify risks, recognize countermeasures, communicate analysis
- Understand ethical, legal, security, and social aspects of the problem and solution
- Also available as on-campus major or minor

SANS

online and in person

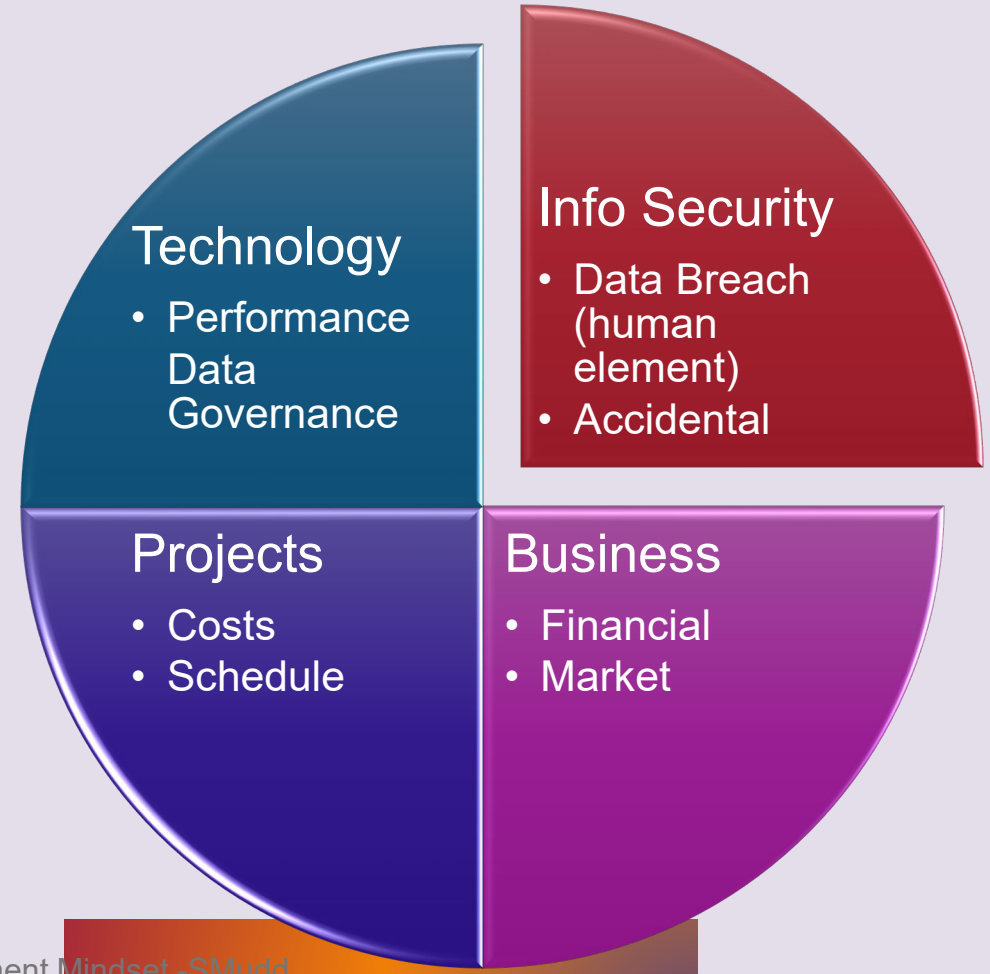
Training Certification

Cybersecurity Risk Management and Compliance

- 5-day Course addressing how to effectively manage cybersecurity risks and ensure regulatory compliance
- Threat modeling, security frameworks, risk analytics

SAMPLE CURRICULUM

RISK MANAGEMENT IS RISK MANAGEMENT



CURRICULUM IDEAS

In Existing Cybersecurity Course (3rd-4th year) - SAMPLE

Unit 1 – Risk Management Concepts

1. Describe the practice of risk management as a general discipline
2. Evaluate the fundamental concepts of risk management
3. Examine key elements for making risk determinations in IT security
4. Analyze the steps in the risk management lifecycle
5. Communicate clearly and concisely the role of risk management for the practice of IT security

Overall Theme: Risk Management is important for all disciplines to understand. Black & White thinking is harmful.

Interdisciplinary Course – Understanding Risk Management

Unit 1 – Risk Management Concepts

Unit 2 – Risk management vs. Other fields

1. Describe the practices of IT governance, security, and compliance
2. Evaluate the interconnectivity between risk management and other IT practices
3. Examine risk management's role in helping prioritize management decisions

Unit 3 – Understanding/Developing a Controls environment

Unit 4 - Risk Assessment, finding gaps and evaluating for risk

Unit 5 – Threats, what are they and how do you find them?

Unit 6 – Vulnerabilities, do I have them and how to find them?

Unit 7 – Impacts, how to determine risk levels and priorities

Unit 8 – Risk treatments: Mitigate, Accept, Avoid, Transfer

Unit 9 – Reporting, Metrics, Monitoring

Unit 10 – Lessons Learned: Strengthening the Envirionment

RESOURCES

ISO/IEC 2005:2011: No longer available. Updated to ISO/IEC 20000-1:2018
https://www.iso.org/standard/70636.html

NIST 800-12: https://csrc.nist.gov/pubs/sp/800/12/r1/final

Carnegie Mellon University:

- BCSA https://www.cmu.edu/interdisciplinary/academics/bcsa-curriculum.html
- BHA https://www.cmu.edu/interdisciplinary/academics/bha-curriculum.html

Georgetown University SCS: https://scs.georgetown.edu/programs/484/online/online-masters-in-cybersecurity-risk-management/

Indiana University: https://cyberrisk.iu.edu/

Penn State: https://www.worldcampus.psu.edu/degrees-and-certificates/penn-state-online-security-and-risk-analysis-information-and-cybersecurity-bachelor-of-science-degree


EXPENSES
TAX
PROFIT
INCOME
ANALYSIS
POLICIES
RULES
SUCCESS

Thank you!!