Risk

UBNetDef SysSec, Spring 2024
Week 11
Lead Presenter: Ray Harenza

Learning Objectives

- Understand analysis fundamentals
- Familiarize with different models of risk decomposition
- Use risk assessment to inform decision making
- Develop meaningful and sound analysis products

Agenda - Week 11

1. **Risk and Analysis Fundamentals**
2. Risk Analysis
3. Production

Risk and Analysis Fundamentals

Definitions, purpose, and point-of-entry

Risk: What is it, and why bother?

- **Risk** - operating SysSec definition:
  - *A degree of exposure that an objective has to negative outcomes*
- Assessing risk well drives informed decision making.
  - In-kind, decisions inform risk assessment.
- Risk is a shared language between executives and specialists.

Who cares about risk?

- Almost every person and organization
  - Ancient and selected for

- Anywhere you're going next
  - Any endeavor that requires resources, public or private:
    - Spend money/time to protect from [x]
    - [y] helps, but there are tradeoffs. Do it?
    - [z] is coming. Do we react?

Risk Analysis: Where did it come from?

- Formal risk analysis is pre-scientific
  - Not inherently repeatable
  - Subject to human intuition and experience
  - *Well* predates mathematics (born circa 600 B.C.)
- Any guesses?
- Risk analysis weighs likelihood against loss
  - Decisions are/were often tactical or logistical
  - Applies to warfighting today in near-original form

Risk factor decomposition

- Risk is decomposed into (at least) two composite factors:
  - **Composite**: multi-part (recall network devices)
  - Two-factor model:
    - "A function of Event *A*'s probability and its consequences"
    - Informal notation: $\text{Risk}_A = f(\text{P}, \text{C})$
    - Quantitative-formal: $\text{R}_A = f(\mathcal{P}(A), \text{C}_A)$

Degrees of exposure? What are those?

- Numbers or words
- **Quantitative**
  - Counted and *never* scored
- **Qualitative**
  - Scored or normative
- **Semi-quantitative**
  - Partially counted, but eventually scored

E.g., $25,000 of risk

E.g., 1,600 lives risked

E.g., 1-Low/Least to 5-High/Most

(See qualitative example)

Qualitative vs Quantitative

Characteristics	Qualitative	Quantitative
Employs complex functions	Less	More
Uses cost benefit analysis	No	Yes
Requires robust data	No	Yes
Requires guesswork	More	Less
Uses opinions	More	Less
Is objective	Less	More
Requires significant time	Less	More
Offers useful results	Hopefully	Hopefully

Agenda - Week 11

1. Risk and Analysis Fundamentals
2. **Risk Analysis**
3. Production

Risk Analysis

Process, factors, tools, and decomposition

Examples of Risk Assessment

- Risk assessments take on myriad of forms and approaches
  - This lecture primarily focuses on IT risk assessments, though many other domains utilize them: finance, military, politics, etc.
- Possible IT risk assessments:
  - Penetration test
  - Business impact analysis
  - Threat modeling
  - Supply chain and Dependency analysis
  - Third-Party vendor assessment
  - Vulnerability assessment
  - Audit of policies, process, procedures
  - Assessment of controls

Analysis: What is it, and why bother?

- **Analysis** – operating SysSec definition:
  - *A formal or semi-formal process of reasoning and communication*
- Formality enables readability for analysis recipients.
  - Recipients are commonly referred to as customers.
- Formality is usually a hassle. When is it beneficial?

Department of
Motor Vehicles

The risk point-of-entry

- Risk assessments are driven by questions from customers.
  - Assessment implies some measure of uncertainty.
- Good risk questions imply an analysis scope.
- Risk assessments provide answers to risk questions.
  - Question quality and analysis quality determine answer quality.
- Who might customers be? What risk questions or decisions might they face?

Differences in risk perspective

- Subject granularity
  - Site Manager vs. Corporate Policymaker
  - Corporate CISO vs. Federal Analyst
- Relevant event timelines
  - Software Engineer vs. Cybersecurity Consultant
- System interdependencies
  - Analyst at Cisco (networking) vs. Analyst at Intel (processors)

Risk perspective

- Where is my analytical position in a system?

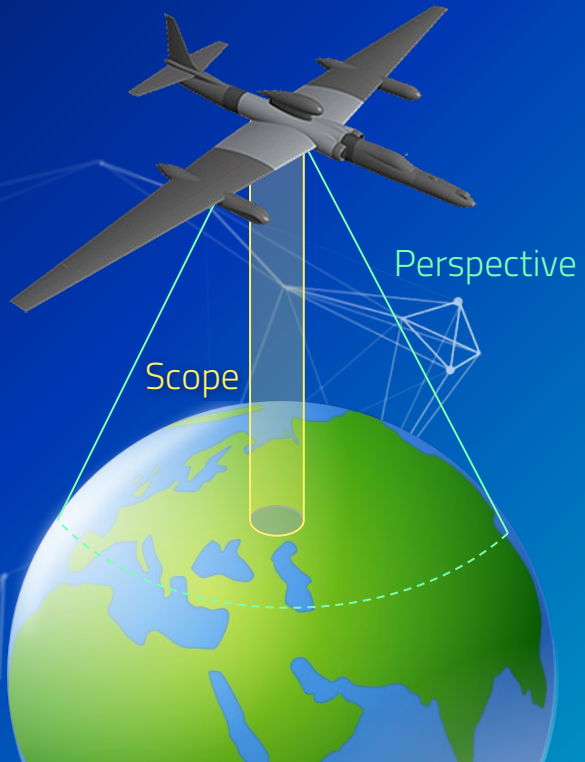
- Decided by the analyst job description:
  - Subject granularity
    - One system? One server room? One corporation? Etc.
  - Relevant event timelines
  - System interdependencies

Risk scope

- Who is this assessment for and what do they want?
- What can be analyzed versus safely ignored?
- When is information relevant versus not relevant?

- Scope is…
  - Informed by the question or decision posed by a customer
  - Decided by agreement between analysts and customers

Perspective and scope illustrated



Risk posture

- How do you determine an organizations risk posture?
  - What is the organization trying to protect?
  - What controls and organizational policies currently exist?

Risk questions

- What perspectives and scope do these risk questions imply?
  - What is the U.S. supply chain risk from foreign cyber attack?
  - How does implementing Graylog affect our company's risk?
  - What Russian tactic is the most catastrophic for Kyiv?

Well-defined analysis environment

- Pointed questions and meaningful constraints
- Analysts can offer focused and informative products:
  - Why risk reflects a customer's current or forecasted state
  - How countermeasures mitigate risk

- Properly assessing existing risk is **good**.
- Anticipating future risk is **better**.
- Handing customers the 'keys' for driving decisions is **best**.

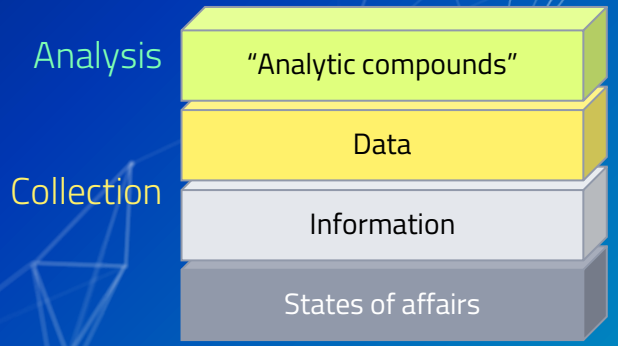
Risk analysis process

- Goal: Assess and communicate risk relevant to a question
- Generally, analysis consists of:
  - **Compilation**
    - Organize data into products for customers.
  - **Dissemination**
    - Deliver products to customersand respond to feedback.

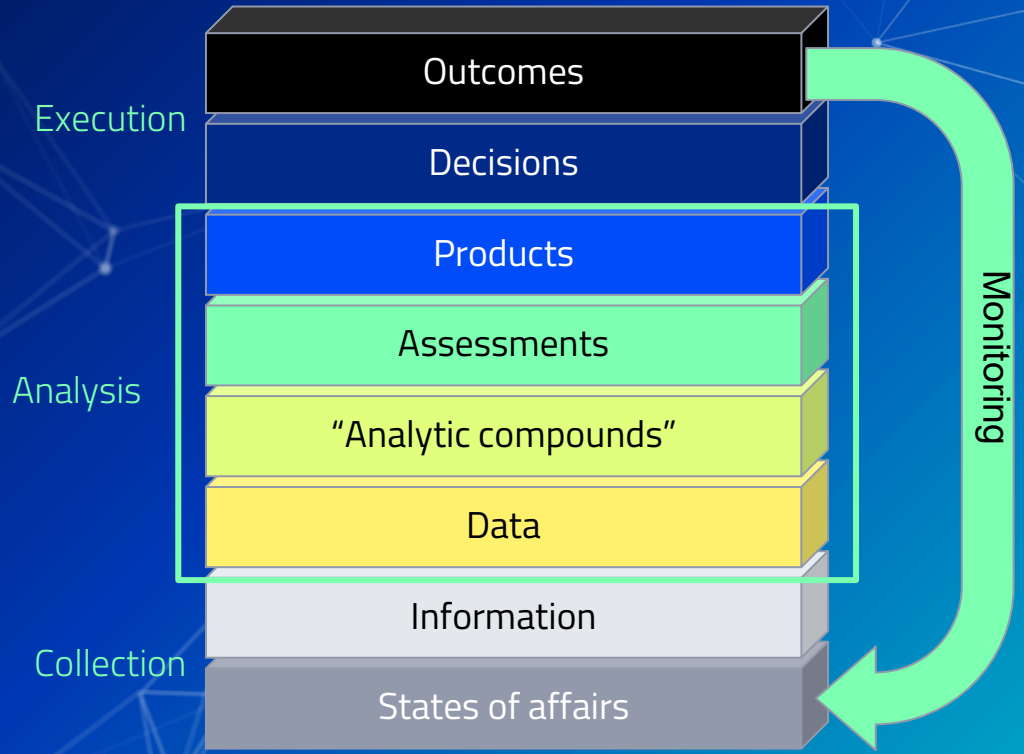
- What (necessarily) comes before compilation?

Data vs Information

- **Information** - operating SysSec definition:
  - Perception of a state of affairs
- **Data** - operating SysSec definition:
  - Organized information formatted for analysis



The analysis stack



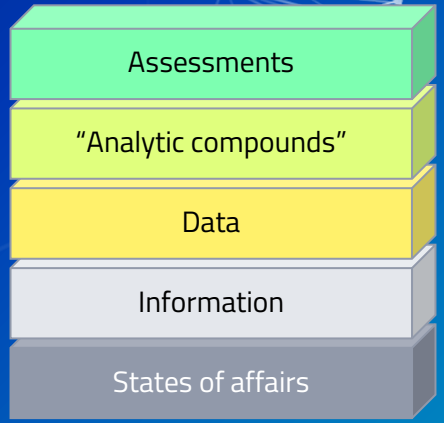
Two-factor risk model at work

- (Negative outcome) Event *A*
  - Has a **roughly even** probability of occurring
  - Has **low-impact** consequences
- Event *B*
  - Has an **unlikely** probability of occurring
  - Has **high-impact** consequences
- Your organization has enough resources to address **one** event.
  - Assume the interventions require the same resources.

"Analytic compounds"

From factors to risk

- From prior:
  - $Risk_A$=(**even**, **low**)
  - $Risk_B$=(**unlikely**, **high**)
- Assessing risk from risk factors needs a further analysis layer:



From factors to risk

- From prior:
  - $Risk_A$=(**even**, **low**)
  - $Risk_B$=(**unlikely**, **high**)
- Assessing risk from risk factors needs a further analysis layer:
  - A risk assessment matrix - see this example:

		Consequences		
		Low	Moderate	High
Probability	Likely	Avoid	Risky	
	Even	A	Avoid	Risky
	Unlikely	Ignore	Notable	B

Risk factor decomposition II

- Recall that risk is decomposed into factors:
  - Three-factor model:
    - Still a probability and consequence function
    - However, probability is further decomposed into Threat and Vulnerability factors[1]
    - Informal notation: $\text{Risk}_A = f(T, V, C)$
- We will leverage the following exercise to explain more:

[1] Threat and vulnerability factors will be defined in the following in-class exercise.

In Class Activity

Qualitative Risk Assessment Part 1

Exercise details

- Complete the exercise: “Commute to UB”
- Consult this risk register:

		Consequence							
		Trivial	Noticable	Moderate	Significant	Destabilizing	Hazardous	Dangerous	Catastrophic
Probability	Imminent	1	3	5	6	7	8	9	10
	Very Likely	1	3	5	6	7	8	8	9
	Likely	1	3	5	6	7	7	8	8
	Rougly even	1	2	4	5	6	7	7	8
	Unlikely	1	2	3	4	5	6	6	6
	Very unlikely	1	2	3	3	3	4	4	4
	Trivial	1	1	1	1	1	1	1	2

Break slide

Please return on time!

Decomposing the Threat Factor

- The exercise in-class evaluates a hazard threat component.
- Human threats can be further decomposed:
  - T = f(Capability, Intent)
    - **Capability**: Likelihood of exploiting existing vulnerabilities
    - **Intent**: Likelihood of seeking defended assets

How do you assess a threat?

- Intensity, timing and diversity of a threat
- Threat actor tools, tactics and procedures
- Threat actor capability, and intent

Data sources: Threats

- Threat information is often considered "Intelligence"
  - Identifies malicious actor category activity
    - E.g., organized crime, hacktivists, etc.
  - Identifies Advanced Persistent Threat (APT) groups
  - Establishes historic targeting and intent
  - Outlines Tactics, Techniques, and Procedures (TTPs)

- Sources:
  - MITRE, Dragos, IBM X-Force

How is threat intelligence useful?

- Depends on the information
  - How useful is knowing a malicious IP
  - How useful would knowing a specific tool the threat actor uses?
- Recent SSH backdoor
  - CVE-2024-3094

How do you discover a vulnerability?

- Vulnerability scanning
- Penetration testing
- Security audits and assessments
- Incident response
- Many more…

How do you rank a vulnerability?

- What is the location of the device in the network?
- How long has the vulnerability been known for?
  - How well documented is exploiting the vulnerability?
- What tools were used to exploit the vulnerability, are tools necessary?
- Is the vulnerability able to be exploited remotely by anyone?
- Is it necessary to have user-level access on the device?
  - What permissions does the user need to exploit the vulnerability on the device?

How do you anticipate future risk?

- Model it
  - Often uses software
- Risk scenario planning
  - Top-down risk scenarios
  - Bottom-up risk scenarios
- Trend analysis
  - How is the regulatory landscape changing?

Data sources: Vulnerabilities

- Vulnerability repositories
  - Source: MITRE CVE
- Scans
  - Sources: Open-VAS, OWASP-ZAP, Rapid7 Nexpose
- Audits
  - Identifies People, Process and Technology (PPT) vulnerabilities.
  - Methodology organized by frameworks. E.g., NIST, ISO

Information and Data sources: Consequences

- Informed by asset value and scope
  - Where are consequence considerations for a …
    - Software engineer?
    - A small business IT manager?
    - A Fortune 500 corporation CISO?
    - A U.S. critical infrastructure security analyst?

- Sources (variable per organization):
  - Supply chain and dependency analyses
  - Historic data
  - Subject matter expertise

How do you measure potential consequences?

- What is a bad actor able to do once the vulnerability is exploited?
  - Is a bad actor able to gain sudo access?
  - Is the bad actor able to impact the integrity of the device or database?
  - Is the bad actor able to view data or terminate a service?
- How does this impact other parts of the organization?
- Can the impact be measured?

What about that gray area?

- How do you evaluate an accident with regards to a risk model or equation?
- How do you handle modeling the location of a device on a network as a vulnerability and a consequence?
- Can AI be a threat or vulnerability?
  - What types of consequences can be driven by AI?

In Class Activity

Created a Prioritized List

Exercise Details

- Complete the exercise: “Create a prioritized list”
- Consult this risk register:

		Consequences			
		Trivial	Noticable	Moderate	Significant
Probability	Very likely	1	3	5	6
	Likely	1	3	4	5
	Roughly Even	1	3	3	3
	Unlikely	1	2	2	2
	Very Unlikely	1	1	1	1

Break slide

Please return on time!

Quantitative assessment in business

- Recall quantitative-formal notation: $R_A = f(\mathcal{P}(A), C_A)$
  - By the probability definition, $0 \leq \mathcal{P}(A) \leq 1$
  - If 1, (Event) *A* is imminent
  - If 0, *A* is impossible
- Let C_A indicate a predicted loss of $50.
  - If *A* is imminent, then you lose $50
  - If *A* is impossible, then you lose $0
  - What if *A* has a 0.5 probability?

Cost/probability bases

- Probability doesn't change outcomes
  - Either *A* happens or it doesn't. *A* doesn't half-happen.
    - I.e., lose $50, or $0, but losing only $25 to *A* is impossible
    - Now, adjust the scope.
- Allow enough time to manifest 1000 event *A* potentials:
  - "More than likely," the organization is looking at ~$25,000 of loss.
  - So, R_{A1000}=`(0.5,$50000)`=`$25000`.
  - Represents '*$25000 risked*' or 'an exposure factor of *25000*.'

Cost/probability bases

- A quantified risk output can (also) be comparative:
  - R_A=25, and R_B=30 -*and*-
  - *A* and *B* are exclusive.
  - Let it be *A* then!

- A quantified risk output can yield on-its-face fiscal advice
  - R_{A100}=$2500 and the mitigation to avoid it is $1000.
    - Do it!

Cost/probability bases

- The summary of the previous discussion:
  - If risk analysis reliably occurs over a long enough period of time:
    - $R_A = f(\mathcal{P}(A), C_A)$ such that $f(x, y) = x * y$
    - English version: Just multiply 'em!
      - Nice.
- However, it's not always so straightforward.

Special case: Lottery problem

- Coarse methodology gets fuzzy around the edges.

- Consider a lottery ticket risk assessment:
  - You pay $1 to win $600M
  - Your ticket has 1/300M probability of winning.
    - ‘Reverse-risk’ is expected value.
    - Expected value on a $1 ticket is $2!
    - …but, the cashier doesn’t just hand you a 2nd dollar.

Special case: Lottery problem

- You *probably* need to buy 300M tickets to win once.
  - Called “realizing your equity”
- You won’t, and if you don’t win, you only donate.
  - This is where the lottery prize pool comes from.
- Both tickets per customer -*and*- winning events aren’t exclusive.
- Good expected value, bad deal.
  - Don’t do it!

The lottery problem analogized

- You can shield your money-making server for $150k
- Your nuclear attack risk assessment yields

$$R_{NUKE} = (0.00001, \$25B) = \$250k$$

- What is your decision?

Agenda - Week 11

1. Risk and Analysis Fundamentals
2. Risk Analysis
3. **Production**

Production

Communication of risk

How do you communicate while writing?

- Create products that are:
  - Well-written
  - Authoritative
  - Reasonable

Know who you are writing to

- Always tailor products to respond to a distinct audience.
  - Ideally, a product audience is a customer that asked an initial analytic question.

- High-value writing rule #1:
  - Anticipate the worst; write to an audience that is:
    - Lazy *-and-*
    - Mean *-and-*
    - Stupid
  - Dr. Dennis Whitcomb, Dept. of Philosophy, Western Washington Univ.

SysSec writing

- Distinct SysSec content audiences:
  a. Intending to replicate a process
  b. Care about an analysis endstate
  c. Need to evaluate analysis details

- What products or product sections correspond to each above?

SysSec writing continued

- Instructional reports show and explain steps
  - Methodical and chronologically ordered
  - Explain *what* to do and *how* to do it.
  - Avoid paragraphs about *why*.
- Informational reports communicate findings or assessments
  - Lead with the conclusion and prioritize impact
  - Provide *what* you found or assess and *why* it matters.
  - Avoid telling a story about *what* you did or *how* you did it.

Enough style guides already!

- Product formality is often managed by style guides.
  - Expect many changes across organizations.

- Consistency helps customers anticipate information.
  - Readers have finite mental bandwidth.
  - Good form helps content stand out.
    - Imagine writing an engaging fictional story…
      - …to register for classes every semester

Final statements

- Professional audiences:
  - ...often lend credibility
    - Writers are adequately credentialed
    - Content is rational and consistent
  - ...may deduct 100% of that credibility instantly or arbitrarily
    - Spelling, grammar, style, tone
    - Controversial or overconfident analyses
    - Poor argumentation or self-contradictory content


Parting questions
Now is the time!

Wrap-up

- Introduced analysis fundamentals
- Reviewed different models of risk decomposition
- Reviewed qualitative and quantitative analysis models
- Described how risk analysis informs decision making
- Outlined good practices for developing analysis products

Class dismissed

See you next week!

Special Thanks to Phil Fox!

MM: @xphilfox | github.com/pcfox-buf | pcfox@buffalo.edu | philip.fox@cisa.dhs.gov