Risk Analysis & Management

UBNetDef SysSec, Fall 2023
Week 10
Lead Presenters:
Ray Harenza
Lauren Moore

Learning Objectives

- Understand analysis fundamentals
- Familiarize with different models of risk decomposition
- Assess data qualitatively and quantitatively
- 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. Risk Management
4. Production

Risk and Analysis Fundamentals

Definitions, purpose, and point-of-entry

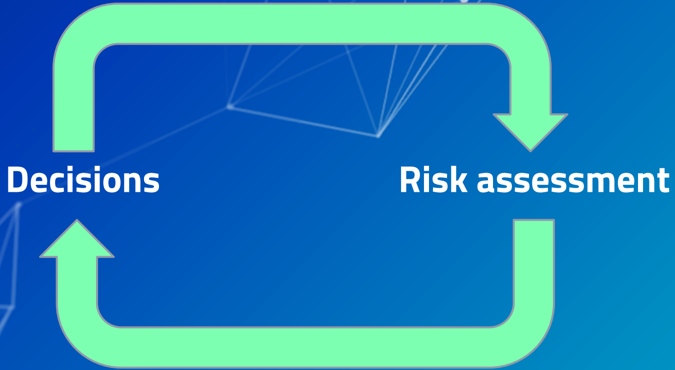
Who cares about risk?

- Almost every person
  - Ancient and selected for
  - You: Register for classes with no guarantees
  - Your parents/guardians: You

- 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: 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.



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?

NEW YORK STATE OF OPPORTUNITY. | Department of Motor Vehicles

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

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)

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?

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

Differences in risk perspective

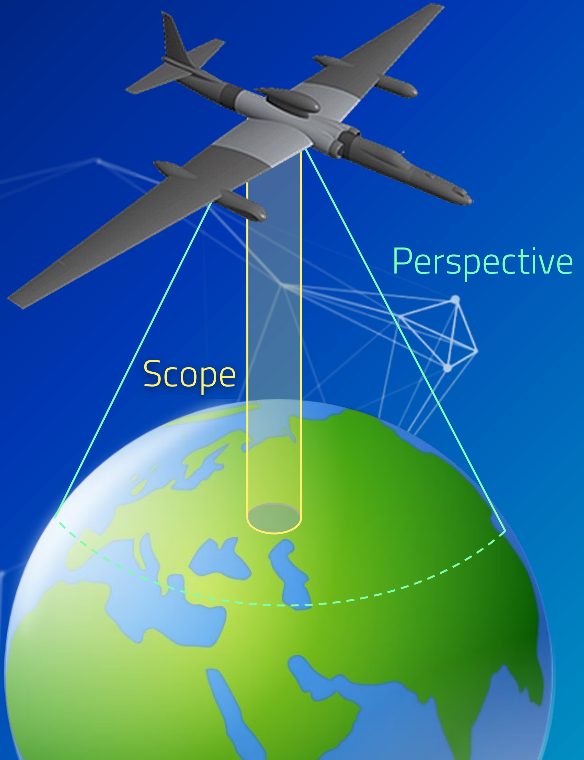
- Subject granularity
  - Site Manager vs. Corporate Policymaker
  - Corporate CISO vs. Federal Analyst
- Relevant event timelines
  - Software Engineer vs. Cybersecurity Consultant
- System interdependencies
  - Analyst at Cisco (networking) vs. Analyst at Intel (processors)

Risk scope

- Who is my customer 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



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 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?

More risk questions

- What perspectives and scope do these risk questions imply?
  - Is my company at risk?
  - What should our company do about Log4j?
  - What are the risks to U.S. critical infrastructure?

Break slide

Please return on time!

Agenda - Week 11

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

Risk Analysis

Process, factors, tools, and decomposition

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 customers and respond to feedback.

- What (necessarily) comes before compilation?

Risk Posture

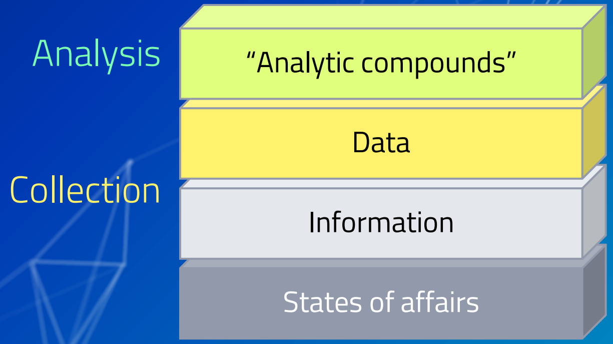
- How do you determine an organizations risk posture?
    - What are is the organization trying to protect?
    - What controls and organizational policies currently exist?
    - Who is responsible for determining risk appetite?

A risk assessment could include the following things

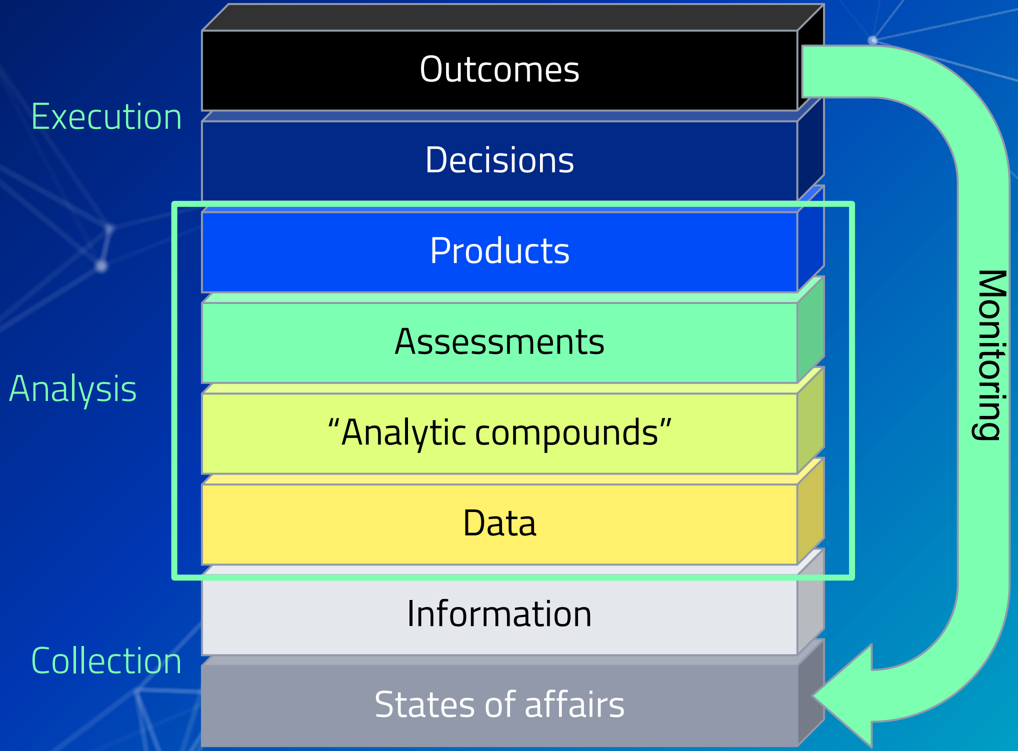
- Penetration test.
- Audit of policies, process, procedures.
- Assessment of controls.
- Vulnerability scan.

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



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: $\text{Risk}_A = f(P, C)$
    - Quantitative-formal: $R_A = f(\mathcal{P}(A), C_A)$

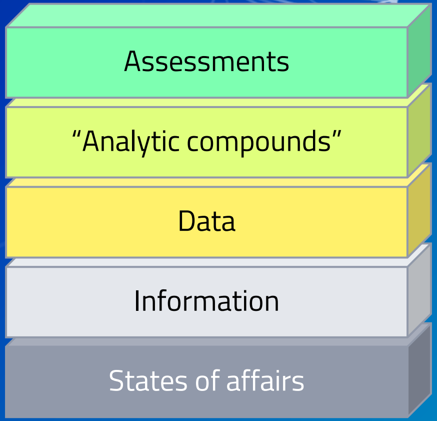
Two-factor risk model at work

- (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”

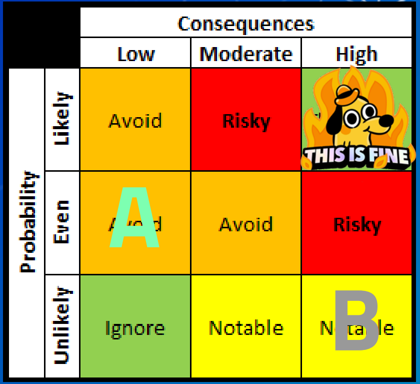
From factors to risk

- 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:

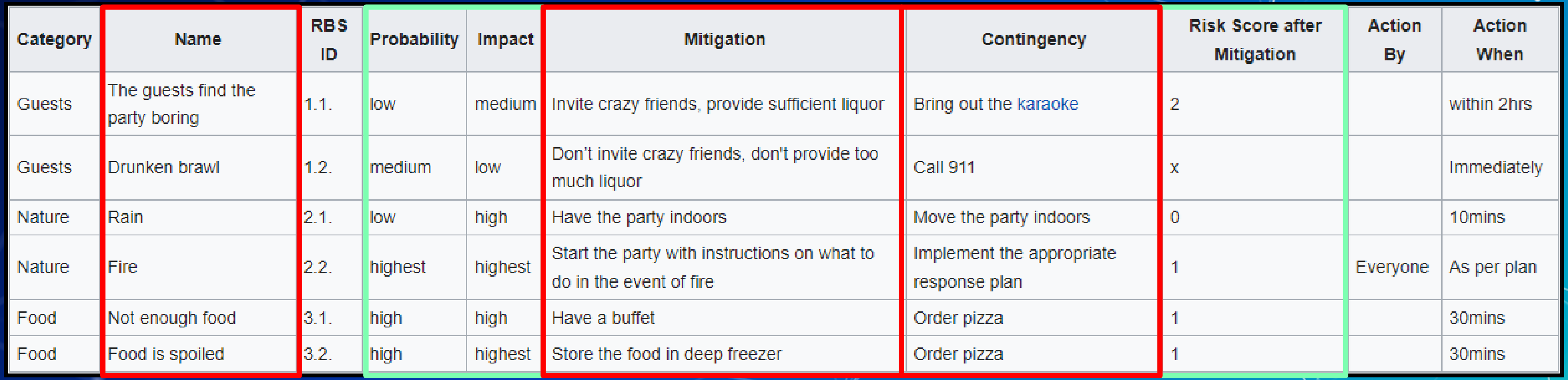


		Consequences		
		Low	Moderate	High
Probability	Likely	Avoid	Risky	THIS IS FINE
	Even	A Avoid	Avoid	Risky
	Unlikely	Ignore	Notable	B Notable

Risk assessment matrix? Where did that come from?

- Executives provide or work together with analysts to define
- Often complicated (they should be!)
- May include risk management factors within the register
  - **Risk Management**: Applied risk analysis
    - Often business-facing
  - Wikipedia provides a good example implementation:

Risk register models



Category	Name	RBS ID	Probability	Impact	Mitigation	Contingency	Risk Score after Mitigation	Action By	Action When
Guests	The guests find the party boring	1.1.	low	medium	Invite crazy friends, provide sufficient liquor	Bring out the karaoke	2		within 2hrs
Guests	Drunken brawl	1.2.	medium	low	Don't invite crazy friends, don't provide too much liquor	Call 911	x		Immediately
Nature	Rain	2.1.	low	high	Have the party indoors	Move the party indoors	0		10mins
Nature	Fire	2.2.	highest	highest	Start the party with instructions on what to do in the event of fire	Implement the appropriate response plan	1	Everyone	As per plan
Food	Not enough food	3.1.	high	high	Have a buffet	Order pizza	1		30mins
Food	Food is spoiled	3.2.	high	highest	Store the food in deep freezer	Order pizza	1		30mins

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:

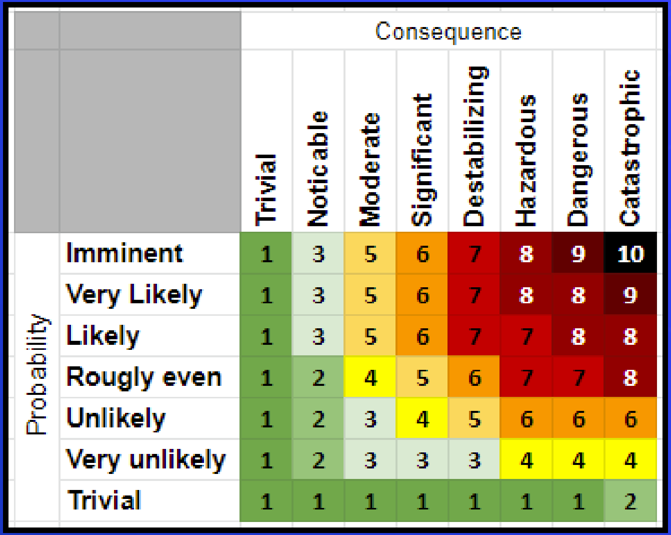
[1] Threat and vulnerability factors will be defined in the following in-class exercise.

In Class Activity

Qualitative Risk Assessment Part 1

Exercise details

- Complete only exercises 1 and 2: “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

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

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

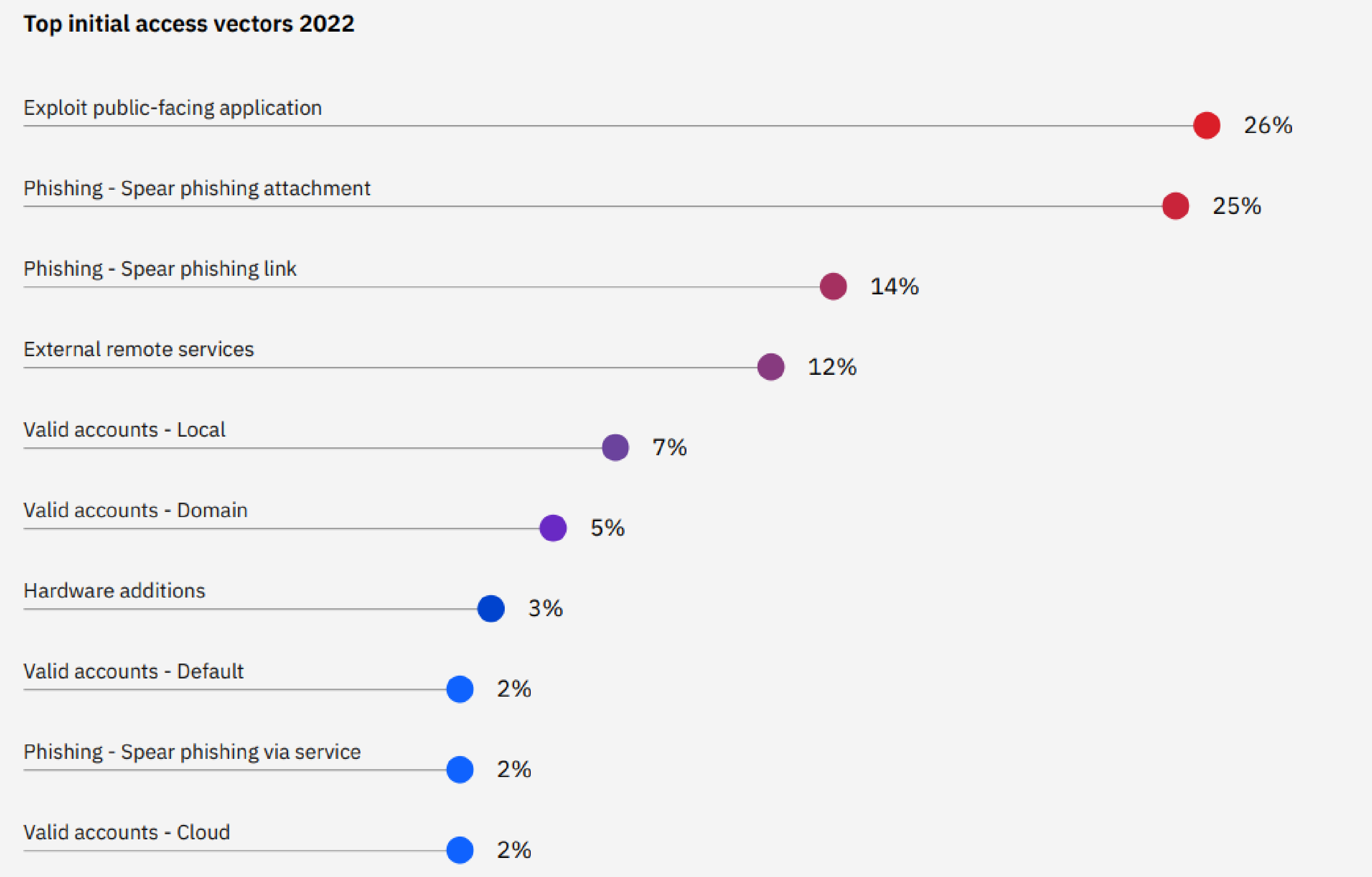


Figure 1: Top initial access vectors X-Force observed in 2022. Source: X-Force

Top actions on objectives 2022

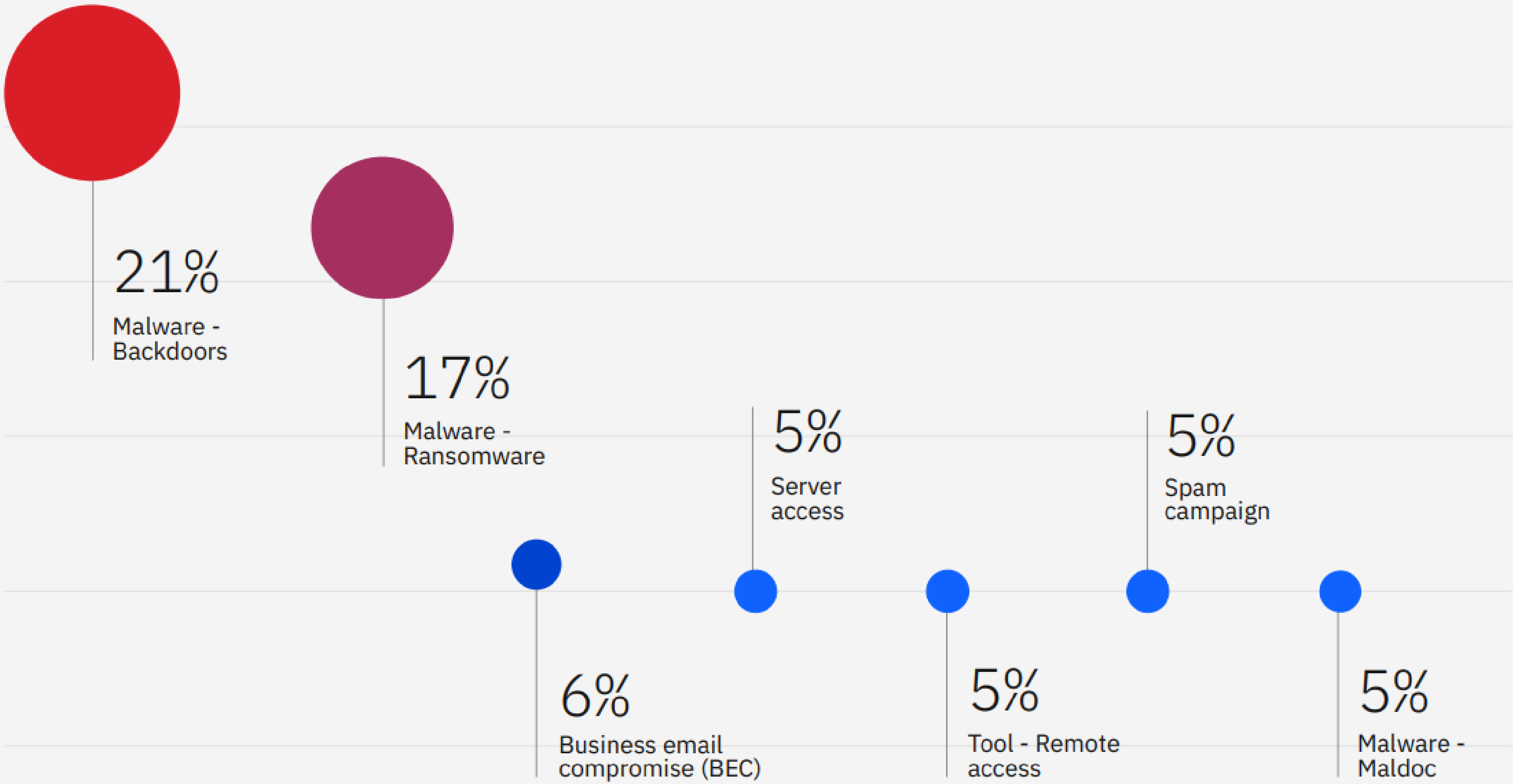


Figure 7: Top actions on objectives observed by X-Force in 2022. Source: X-Force

Top impacts 2022

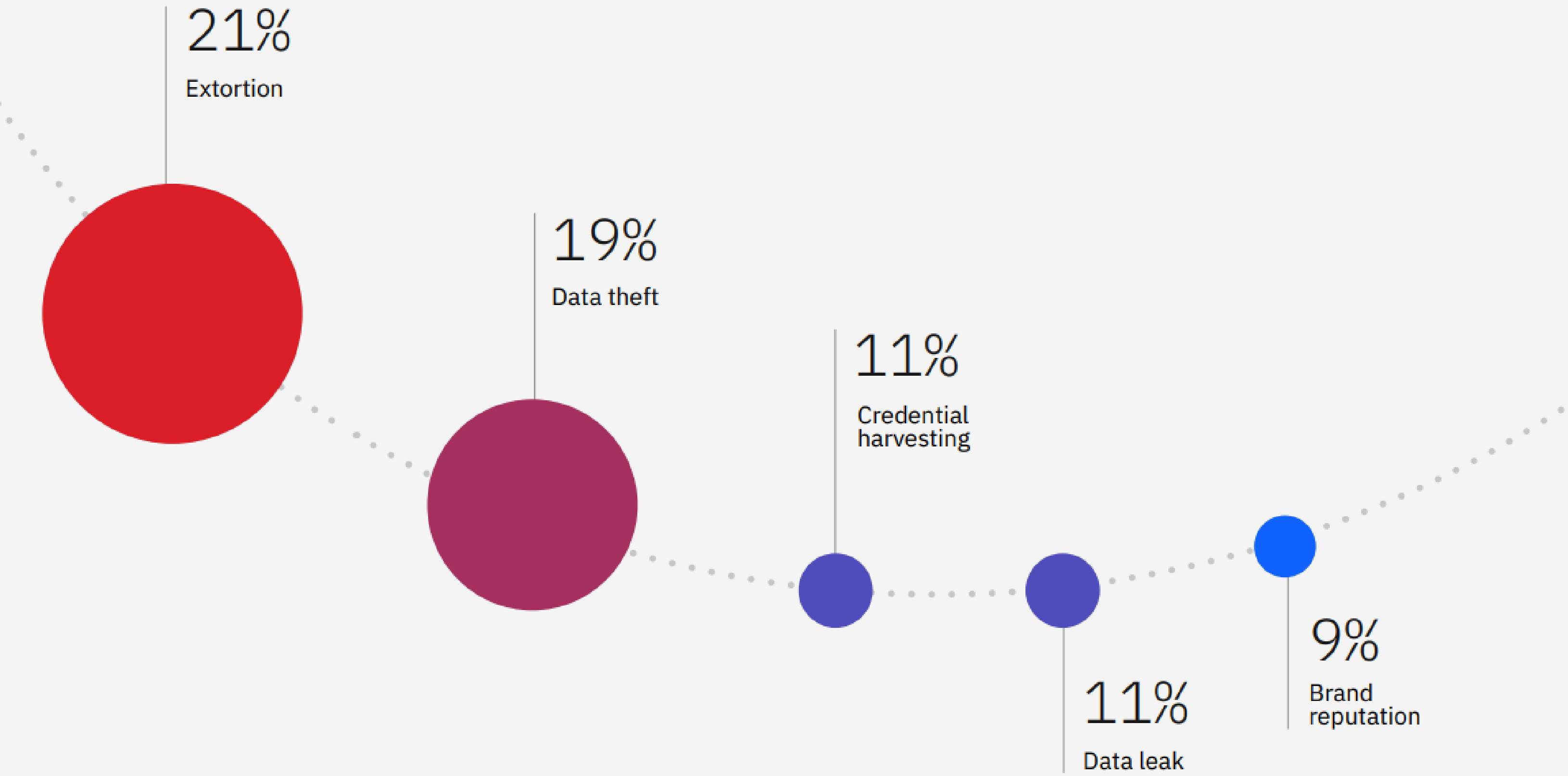


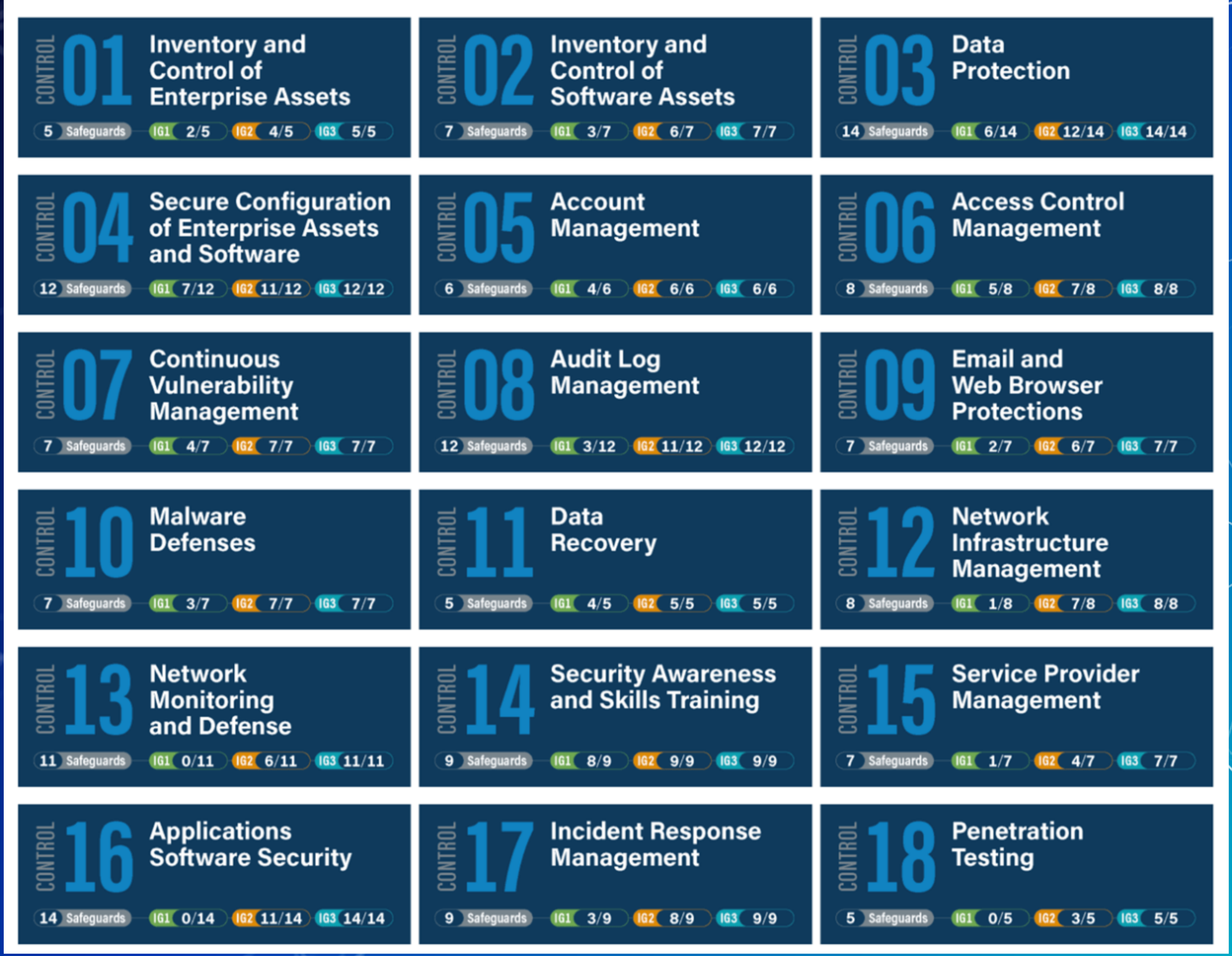
Figure 10: Top impacts X-Force observed in incident response engagements in 2022. Source: X-Force

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



CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7	CONTROL 03 Data Protection 14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12	CONTROL 05 Account Management 6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6	CONTROL 06 Access Control Management 8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8
CONTROL 07 Continuous Vulnerability Management 7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7	CONTROL 08 Audit Log Management 12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12	CONTROL 09 Email and Web Browser Protections 7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7
CONTROL 10 Malware Defenses 7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7	CONTROL 11 Data Recovery 5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5	CONTROL 12 Network Infrastructure Management 8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8
CONTROL 13 Network Monitoring and Defense 11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11	CONTROL 14 Security Awareness and Skills Training 9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9	CONTROL 15 Service Provider Management 7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7
CONTROL 16 Applications Software Security 14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14	CONTROL 17 Incident Response Management 9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9	CONTROL 18 Penetration Testing 5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

Center for Internet Security (CIS) Controls Framework v8

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

Break slide

Please return on time!

Agenda - Week 11

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

Risk Management

Quantitative assessment and empowering decision-making

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.

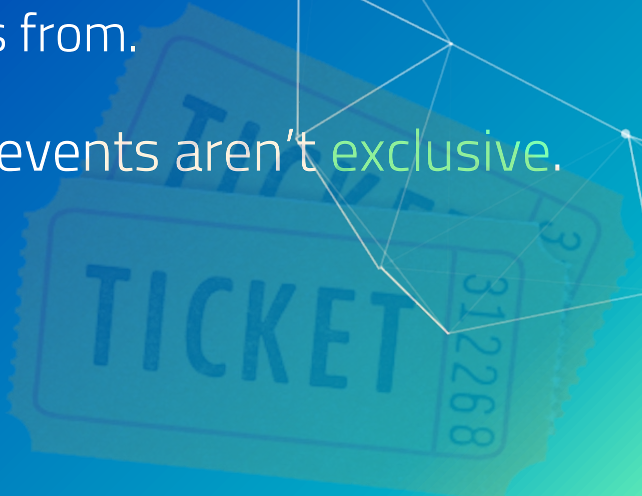
Special case: Lottery problem

- 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

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

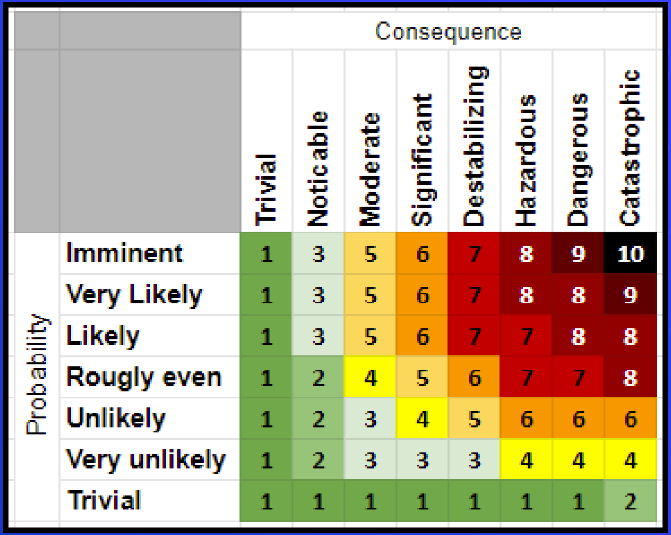
- What is your decision?

In Class Activity

Qualitative Risk Assessment Part 2

Exercise details

- Complete remaining exercises 3 and 4: “Attend Remote”
- 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

Risk assessment at business scale

- Several quantitative models exist that modify scope.
  - May scale across longer periods of time
  - May constrict or expand across systems

- New model: Annualized Loss Expectancy (ALE)[1]
  - Which part of the acronym signals a scope change from prior?

[1] Note that this is one of *several* formula models. Find more re: incident response, and others from information assurance or game theory classes, textbooks, etc.

Traditional ALE decomposition

- ALE:
  - Annualized Rate of Occurrence (ARO)⋆Single Loss Expectancy (SLE)
    - ARO:
      - Expected count of exploited vulnerabilities per year
    - SLE:
      - Exposure Factor (EF)⋆Asset Value (AV)
        - EF:
          - *How much* of the asset is lost on exploit? [0,1]
- So, ALE=EF⋆Asset Value⋆ARO
  - = How much we stand to lose in a year.
  - Is ALE Qualitative or Quantitative?

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

Executive risk considerations

- Recall that mitigations reduce risk.
  - Also known as countermeasures or controls
  - Mitigate what in particular?
- Residual risk:
  - Risk left over in light of existing or anticipated controls
- Assuming residuals exist (usually do) what next?

Executive risk considerations

- Appetite
  - I.e., tolerance
  - High appetite versus low appetite
    - How does this manifest in an organization?
- Offloading
  - Insurance
  - System distribution/migration

Evaluate and Monitor

- Discovering insufficient controls
  - Result of an audit
  - Something goes wrong
  - Constant Monitoring

How do different size organizations manage risk?

- Frameworks
  - Varies for different organizations
- CIS Critical Security Controls

Agenda - Week 11

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

Production

Rhetoric and dissemination

What is rhetoric, and why does it matter?

- **Rhetoric** - operating SysSec definition:
  - *Artful, persuasive communication*
  - Edifies "the customer is always right" principle

- Rhetoric decomposed, translated:
  - Well-written
  - Authoritative
  - Reasonable

Applied ‘pathology’

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

- High-value ‘pathological’ 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.

Applied ‘pathology’

- 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?

Applied ‘pathology’

- 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

Applied ‘ethics’ and logic

- 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

Dissemination

- Coordinate
  - Ask for feedback; adjudicate; press on
  - **Adjudication**: 'apply it or not'
- Collaborate
  - Ask for feedback; revise; agree
- Best Practices
  - Communicate deadlines to partners
  - Ask partners for feedback time requirements
  - Provide advance notice for missed deadlines
    - Don't miss deadlines

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

Homework prep

Pending remaining class time

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