Project #1: Security Breach Communication & Persuasion Video

Secure System Engineering and Management

Due date: Tuesday, February 9
Format: Pre-recorded video presentation (10–15 minutes)
Weight: Part of the Projects component (40% total across five projects)

Project Overview

In this project, you will analyze a **real-world cybersecurity breach** and present it as a **persuasive briefing to organizational leadership**. You will take the role of a cybersecurity expert whose job is not merely to explain what happened, but to **convince decision-makers to invest in security changes** that would reduce the risk of a similar breach in the future.

This is a **communication-focused assignment**. A technically accurate summary is necessary but not sufficient. Your goal is to demonstrate that you understand:

- **Why** the breach happened (technical, organizational, and human causes),
- **What** could realistically have reduced the risk,
- **How** to communicate those lessons persuasively and empathetically to non-expert stakeholders with competing priorities.

Breach Selection

You must choose **one breach** from the following resource:

> **World's Biggest Data Breaches & Hacks**
> `https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/`

You may choose any breach listed on the site, regardless of industry or year, provided there is sufficient public reporting to support your analysis.

Important: Avoid breaches where the takeaway is trivial (e.g., "they should have patched sooner"). Choose a case with meaningful technical, organizational, or human lessons.

Audience and Framing (Very Important)

Your intended audience is **company leadership** (e.g., executives, board members, senior managers).

Assume that your audience:

- Is intelligent but **not security-expert**,
- Cares about **business continuity, cost, reputation, compliance, and risk**,
- May be skeptical of security spending,
- Did not cause the breach, but controls future investments.

Your presentation should:

- Avoid unnecessary jargon,
- Explain technical issues clearly and visually,
- Use evidence **and** empathy,
- Frame recommendations in terms leadership can accept.

Think: *"If I were the CISO or senior security engineer, how would I explain this so it actually changes decisions?"*

Deliverable Requirements

1. Video Presentation (10–15 minutes)

Your video should tell a **coherent story**, not a list of facts. A strong structure might include:

A. Context and Stakes (≈ 1–2 minutes)

- What organization was breached?
- What kind of organization is it (industry, scale, mission)?
- What assets were affected (data, systems, people)?
- Why leadership should care (impact on users, finances, trust, operations)?

B. What Happened (≈ 2–3 minutes)

- High-level timeline of the breach,
- How the attack worked (at the right level of abstraction),
- Where humans, processes, and technology interacted.

Avoid excessive technical depth unless it directly supports your later arguments.

C. Root Causes and Contributing Factors (≈ 3–4 minutes)

Go beyond "the vulnerability":

- Technical causes (e.g., design flaws, missing controls),
- Organizational causes (e.g., incentives, tradeoffs, technical debt),
- Human factors (training, workload, usability, attacker behavior),
- Why these failures were **plausible** in context.

D. Persuasive Mitigations and Recommendations (≈ 4–5 minutes)

This is the **core of the project**.

You should:

- Propose **specific, realistic mitigations**,
- Explain how they would reduce risk,
- Address tradeoffs (cost, complexity, disruption),
- Prioritize recommendations,
- Explicitly connect recommendations to lessons from the breach.

Consider mitigations related to secure design, development practices, operations, monitoring, response, and human-centered interventions.

E. Closing: The Big Picture (≈ 1 minute)

- What leadership should take away,
- Why investing now is better than reacting later,
- How this breach generalizes beyond one company.

2. Slides and Visuals

- Slides should **support the narrative**, not replace it,
- Diagrams are strongly encouraged (attack paths, system architecture, defenses),
- Avoid dense bullet lists,
- Visual clarity matters. (We should be able to clearly see you in the video.)

3. Submission Instructions

Submit the following on Canvas:

- A link to your video (please provide an unlisted YouTube video link),
- A PDF of your slides.

Videos must be **10–15 minutes** in length (with a ±1 minute grace).

What This Project Is Not

- Not a Wikipedia-style breach summary,
- Not a purely technical deep dive with no persuasion,
- Not a list of generic best practices,
- Not a hindsight-driven blame exercise.

Use of Generative AI Tools

Students are permitted to use generative AI tools (e.g., large language models) to assist with:

- Understanding the details of a breach,
- Exploring possible interpretations or contributing factors,
- Brainstorming ways to frame explanations or recommendations.

However, the submitted presentation must reflect **your own understanding, judgment, and communication**. In particular:

- Do not copy or directly reuse AI-generated text or scripts,
- Do not outsource analysis or recommendations to an AI system,
- Be prepared to explain and defend your choices and conclusions.

This project emphasizes **independent thinking, synthesis, and persuasive communication**. Over-reliance on generative tools will be reflected in the grading, particularly in categories related to insight, clarity, and delivery.

Grading Rubric (35 points total)

Each category is scored on a **0–5 scale**, for a total of **35 points**. Presentation Quality and Delivery will be emphasized in grading, particularly given the communication-focused goals of this project.

Category	**Criteria**
Understanding of the Breach	Depth and accuracy of technical and contextual understanding
Thoughtfulness & Insight	Goes beyond headlines; original analysis and reasoning
Context & Perspective	Organizational, economic, and human factors clearly integrated
Persuasiveness of Recommendations	Specific, realistic, prioritized, and well-argued mitigations
Communication & Empathy	Clear, empathetic, appropriate for leadership audience
Clarity & Organization	Strong narrative flow and clear big-picture framing
Presentation Quality & Delivery	Polished, well-practiced delivery; effective pacing; clear and professional visuals; strong evidence of preparation and ownership of the material.

Final Notes

This project is an opportunity to practice a **core professional skill in cybersecurity**: explaining risk and advocating for change in a way that others can accept. The strongest submissions will not only show that you understand security, but that you understand **people**.