Extension: Executive Briefing Challenge

Translating Technical Findings for Non-Technical Audiences

Dr. Ryan Straight

2025-12-07

> ❗ **Instructor Overview**
>
> This extension activity challenges students to translate technical security findings into clear, actionable communication suitable for non-technical stakeholders. The exercise develops what practitioners recognize as one of the most consequential competencies in cybersecurity careers: the capacity to render complex technical analysis accessible to decision-makers whose expertise lies in other domains. Students discover through practice that technical proficiency, however sophisticated, achieves organizational impact only when paired with effective communication across disciplinary boundaries.
>
> **Duration**: 25-35 minutes (standalone) or integrated into Activity 1 or 3 debrief **Recommended Use**: After completing Security Detective Teams or SOC Analyst Simulation **Grade Levels**: Primarily 9-12, adaptable for 6-8 **Technology**: Word processor or pen/paper

Learning Objectives

Through completing this challenge, students will develop facility in translating technical findings into accessible language while preserving analytical accuracy, distinguishing between information non-technical stakeholders need to know and information of secondary relevance, and applying executive summary writing conventions appropriate to organizational contexts. Students will recognize audience analysis as an essential security communication skill and understand how communication competency functions as a determinant of career advancement in cybersecurity fields.

NICE Framework Connection

- **Technical Writing**: Documenting technical information for various audiences
- **Cybersecurity Management**: Communicating with organizational leadership
- **Security Awareness**: Explaining security concepts to non-specialists

The Challenge

Your Assignment

You have just completed an investigation (from Activity 1 or 3). Your technical findings are solid, but now comes the harder part: explaining them to the principal.

Principal Martinez's Profile:

- Former English teacher, now school administrator
- Excellent with people, budgets, and policy
- Limited technical background (knows how to use email and spreadsheets)
- Responsible for communicating with parents, school board, and media
- Needs to make decisions about resources and response

Your Task: Create a one-page Executive Briefing that Principal Martinez can:

1. Understand completely in under 3 minutes
2. Use to answer parent questions
3. Base resource decisions on
4. Share with the school board if needed

Executive Briefing Template

One-Page Format

```
EXECUTIVE BRIEFING: [Incident Title]
Date: [Date]
Prepared by: [Your Team Name]
Classification: [Internal Use Only / Confidential]



SUMMARY (2-3 sentences)
What happened, in plain language. No jargon.



IMPACT
• Who/what was affected
• What information was at risk
• Current status



HOW IT HAPPENED (simplified)
Brief, non-technical explanation of the incident chain.



ACTIONS TAKEN
  Immediate steps completed
→ Steps currently in progress
  Planned next steps



DECISIONS NEEDED
```

What does Principal Martinez need to decide or approve?

TALKING POINTS (for parent questions)
- If asked about [topic]: [suggested response]
- If asked about [topic]: [suggested response]

Contact: [Your team] | Next Update: [Date/Time]

Translation Guide

Common Technical Terms → Plain Language

Technical	Plain Language
Malware	Harmful software that got on our computers
Phishing	Fake emails designed to trick people
Data breach	Unauthorized access to private information
Lateral movement	The attacker spread from one computer to others
C2 / Command and Control	The attacker's way of controlling infected computers
Credential compromise	Passwords were stolen
Patch / Update	A fix for a known security weakness
Firewall	A digital barrier that blocks unauthorized access
Encryption	Scrambling information so only authorized people can read it
MFA / Two-factor	Requiring two proofs of identity (like password + phone code)

What Executives Need vs. What They Don't

Executives Need	Executives Don't Need
Scope of impact	Detailed log analysis
Timeline of key events	Every technical step taken
Current risk status	IP addresses and hashes
Resource requirements	Tool names and versions
Decisions to make	MITRE ATT&CK framework details
Talking points for stakeholders	Forensic methodology

Grade Band Variations

Grades 6-8: Simplified Briefing

Modified Challenge: Write a "3-Sentence Summary" for the principal:

1. **What happened** (one sentence)

2. **What we did about it** (one sentence)
3. **What happens next** (one sentence)

Then write **one talking point** the principal could use if a parent asks.

Grades 9-12: Full Executive Briefing

Complete the full one-page template. Additional challenge: Present the briefing orally in 90 seconds.

Advanced Extension: Role-Play Presentation

One student presents the briefing while another plays Principal Martinez, asking clarifying questions:

- "Can you explain that in simpler terms?"
- "What should I tell parents?"
- "Do we need to spend money on this?"
- "How do we prevent this from happening again?"

Evaluation Criteria

Executive Briefing Rubric

Criterion	Developing (1-2)	Proficient (3)	Advanced (4)
Clarity	Technical jargon remains	Mostly accessible language	Completely jargon-free without losing accuracy
Completeness	Missing key sections	All sections addressed	Anticipates questions not asked
Actionability	Unclear what executive should do	Clear decisions identified	Specific, prioritized recommendations
Accuracy	Simplification loses important details	Technical accuracy preserved	Complex ideas simplified elegantly
Professional-ism	Informal tone/format	Professional presentation	Executive-ready document

Assessment Connection

Rubric Criterion	Developed Through	Evidence Source
Communication Quality	Translation from technical to plain language	Briefing document clarity score
Audience Analysis	Adapting content for Principal Martinez	Appropriateness of detail level
Professional Judgment	Deciding what to include/exclude	Completeness vs. brevity balance
Synthesis Quality	Distilling complex investigation	Quality of summary section

Applicable Rubrics: Decision-Making Quality Rubric

Career Connection

Why This Matters

Security practitioners often encounter what might be termed the communication ceiling: technical skills secure initial employment, but communication skills determine professional advancement. Numerous talented security professionals experience career plateaus not from technical limitations but from difficulty explaining their work to organizational leaders who lack technical backgrounds.

The real-world context reinforces this pattern across multiple dimensions. Chief Information Security Officers allocate more professional time to communication activities than to technical analysis. Board-level presentations directly determine security budget allocations. Effective incident response necessarily encompasses stakeholder communication alongside technical remediation. Career advancement into leadership roles requires the capacity to exercise influence well beyond the Security Operations Center.

NICE Framework Alignment

This activity develops competencies essential to progression from technical roles into management positions. The relevant NICE Framework work roles include Information Systems Security Manager (OV-MGT-001) with its emphasis on executive communication, Cyber Policy and Strategy Planner (OV-SPP-002) requiring sustained stakeholder engagement, and Executive Cyber Leadership (OV-EXL-001) centered on strategic communication across organizational levels.

Implementation Notes

Connecting to Core Activities

When implemented following the Security Detective Teams activity, students translate their investigation findings into an executive briefing format, concentrating on what the principal genuinely needs to understand about the phishing incident to fulfill administrative responsibilities.

When implemented following the SOC Analyst Simulation, students prepare the executive briefing required in Phase 4 with deliberate emphasis on audience adaptation principles rather than content generation alone.

Common Student Struggles

Students frequently struggle with calibrating appropriate detail levels. Over-explanation manifests when students include excessive technical detail; instructors should encourage students to ask whether the principal needs to understand how the finding was discovered or merely what was found. Under-explanation occurs when students oversimplify to the point of rendering the briefing operationally useless; the document must enable informed decision-making, not merely summarize events. Technical writing habits also carry over problematically, particularly through passive voice constructions. Encourage direct, active language: "An attacker accessed…" rather than "Access was gained by…"

Facilitating Peer Review

Structure peer review around three evaluative questions: Could a reader without technical background understand everything presented? Does the reader know what decisions require attention? Could the reader use this information to address a parent's question?

Low-Resource Option

If technology is limited, provide a completed "technical report" on paper and have students create the executive briefing translation using pen and paper. The core skill—audience adaptation—doesn't require technology.

Sample Technical Input: > Analysis of network logs revealed anomalous authentication patterns consistent with credential stuffing attack. Initial access vector identified as spearphishing email (T1566.001) delivered to finance department at 14:23 UTC. Subsequent lateral movement (T1021) detected across 47 endpoints. C2 beacon established to 185.234.x.x with 20-second interval. Threat intelligence correlation indicates APT29 tooling with MANUFACTURING-AUTUMN campaign TTP alignment.

Student Task: Transform this into language Principal Martinez can understand and act upon.