

Sean Shreve
February 24, 2026
CYSE 200T
Professor Duvall

AI Assignment: What to do with Cybersecurity?

Below is a structured 2–4-page executive-style analysis appropriate for a large publicly traded company.

Organizational Placement of a New Cybersecurity Department

Strategic Analysis of Reporting Structure Options

Executive Summary

The placement of a cybersecurity function materially affects independence, risk governance, operational effectiveness, regulatory compliance, and enterprise resilience. In a publicly traded company—where fiduciary responsibility, regulatory oversight, and shareholder confidence are critical—the reporting structure must align cybersecurity with enterprise risk while preserving operational integration.

This analysis evaluates four placement options:

1. Under Information Technology (IT)
2. Under Finance
3. Under Operations
4. Reporting directly to the CEO

Each structure presents distinct tradeoffs in authority, independence, budget control, and risk alignment.

1. Cybersecurity Under Information Technology (IT)

Overview

Traditionally, cybersecurity has been embedded within IT because IT owns infrastructure, systems, and technical architecture.

Advantages

Operational Alignment

Cybersecurity tools (firewalls, EDR, SIEM, IAM, patch management) integrate directly with IT systems. Close proximity enables:

- Faster incident response
- Better change management coordination
- Efficient vulnerability remediation

Technical Synergy

IT teams understand infrastructure dependencies. Embedding cybersecurity promotes:

- Secure-by-design architectures
- Integrated DevSecOps practices
- Shared tooling and monitoring

Cost Efficiency

Budget consolidation avoids duplicated tools and redundant staffing structures.

Disadvantages

Lack of Independence (Conflict of Interest)

IT builds and maintains systems. Cybersecurity must audit, monitor, and sometimes challenge IT decisions. Reporting into IT may:

- Reduce objectivity
- Create pressure to downplay vulnerabilities
- Lead to “self-policing”

Risk Framing Becomes Technical Instead of Enterprise-Level

Security may be treated as:

- A technical problem
 - A compliance checkbox
- Rather than an enterprise risk issue affecting reputation, regulatory exposure, and shareholder value.

Regulatory Scrutiny Concerns

Public companies increasingly face SEC disclosure requirements around cybersecurity governance. A lack of independence may raise governance questions.

Summary Assessment

Best for operational efficiency, but weaker in governance independence and risk authority.

2. Cybersecurity Under Finance

Overview

Finance owns enterprise risk management (ERM), compliance reporting, and Sarbanes-Oxley (SOX) controls in public companies.

Advantages

Strong Risk & Compliance Alignment

Cybersecurity directly impacts:

- Financial reporting controls
- SOX compliance
- Regulatory penalties
- Breach disclosure obligations

Placement under Finance elevates cybersecurity as a financial risk issue.

Board Visibility

CFOs typically interface directly with audit committees. Security risks may gain:

- Greater transparency
- Stronger reporting discipline
- Clearer metrics and accountability

Budget Discipline & ROI Focus

Finance-driven governance may improve:

- Investment prioritization
- Risk quantification
- Cyber insurance alignment

Disadvantages

Limited Technical Depth

Finance leadership may lack deep cybersecurity expertise, potentially:

- Slowing operational decisions
- Over-emphasizing cost control
- Underestimating technical threat evolution

Operational Disconnect

Security execution requires tight integration with IT and Operations. Finance-based placement may:

Commented [SS1]: I have very little understanding of what a Sarbanes-Oxley is and how its compliance relate to cybersecurity operations in the finance sector of a business. I do understand the other three points made in the list, but SOX compliance is an enigma.

- Create bureaucratic friction
- Delay remediation cycles

Risk of Over-Compliance Focus

Security may become audit-driven instead of threat-driven.

Summary Assessment

Strong governance and financial risk integration, but may weaken technical agility.

3. Cybersecurity Under Operations**Overview**

Operations focuses on service delivery, uptime, manufacturing, logistics, and business continuity.

Advantages**Resilience-Centered Approach**

Modern cybersecurity is not just about prevention—it is about:

- Business continuity
- Incident response
- Disaster recovery
- Operational resilience

Operations alignment supports uptime and service continuity.

Integration with Physical & OT Security

In industries with industrial control systems (ICS) or OT networks:

- Security must align closely with operational technology
- Cyber-physical risk is tightly coupled

Performance-Oriented Execution

Operations tends to emphasize metrics, uptime, and efficiency.

Disadvantages**Potential Risk Blind Spot**

Operations may prioritize productivity over control enforcement. Security controls may be perceived as friction.

Limited Governance Authority

Operations leaders typically do not own enterprise risk reporting to the Board.

Conflict During Incidents

Security may recommend shutdown; operations may resist due to revenue impact.

Summary Assessment

Strong for resilience and business continuity; weaker for governance independence and regulatory posture.

4. Cybersecurity Reporting Directly to the CEO

Overview

In this structure, the Chief Information Security Officer (CISO) reports directly to the CEO or has a dotted line to the Board/Audit Committee.

Advantages

Enterprise-Level Risk Positioning

Cybersecurity becomes:

- A strategic business risk
- A reputational risk
- A shareholder risk

This reflects current SEC and global regulatory expectations.

Independence from IT

Allows security to:

- Audit IT objectively
- Escalate systemic risks
- Challenge operational decisions

Board-Level Governance Alignment

Public companies increasingly expect:

- Direct reporting to audit committees
- Formal cybersecurity oversight

Cultural Signal

Reports directly to CEO communicates:

- Security is a top priority
- Not just a technical function

Disadvantages

Higher Leadership Burden

CEO must meaningfully understand cybersecurity risk to supervise effectively.

Possible Organizational Friction

Without careful design, this model can:

- Create tension with IT
- Duplicate responsibilities
- Blur operational ownership

Requires Mature CISO Leadership

Not all security leaders are prepared for strategic-level reporting.

Summary Assessment

Strongest governance and independence model; requires executive maturity and clearly defined roles.

Comparative Risk Governance Analysis

Placement		Operational Efficiency	Independence	Board Alignment	Risk Framing
IT	High	Low	Moderate	Technical	
Finance	Moderate	Moderate	High	Financial	
Operations	High	Low-Moderate	Low	Continuity	
CEO	Moderate	High	Very High	Enterprise	

Strategic Recommendation for a Publicly Traded Company

Given modern regulatory scrutiny, SEC cybersecurity disclosure rules, and investor expectations:

Best Practice Model:

Cybersecurity should report either:

- Directly to the CEO **or**
- To the CEO with a strong dotted-line relationship to the Board/Audit Committee
- With close operational integration with IT

This hybrid model balances:

- Governance independence
- Operational integration
- Board oversight
- Enterprise risk management

Additional Considerations

1. **Regulatory Environment**
 - SEC cybersecurity disclosure requirements
 - SOX implications
 - Industry-specific mandates (HIPAA, PCI-DSS, NERC-CIP, etc.)
2. **Industry Risk Profile**
 - Technology company vs. manufacturing vs. financial services
 - OT/ICS exposure
3. **Company Maturity**
 - Early-stage cybersecurity programs may initially reside in IT
 - Mature enterprises trend toward independent CISO structures
4. **Three Lines of Defense Model**
 - IT/Operations: First line (execute controls)
 - Cybersecurity: Second line (monitor, govern)
 - Internal Audit: Third line (independent assurance)

Commented [SS2]: It seems this industry is very acronym heavy, much like the military. NERC-CIP and PCI-DSS and SOX are mandates I am not familiar with and I look forward to educate myself on the topic.

Conclusion

The placement of cybersecurity is fundamentally a governance decision, not merely an organizational convenience.

- Under IT → operationally efficient but weaker independence
- Under Finance → strong risk alignment but weaker technical agility
- Under Operations → resilient-focused but governance-light
- Reporting to CEO → strongest strategic and governance model

For a large publicly traded company, where reputational damage, regulatory penalties, and shareholder value are at stake, cybersecurity should be positioned as an **enterprise risk function with direct executive-level visibility and independence**, while maintaining tight integration with IT for operational execution.

Sean Shreve

24FEB2026

Our Company

CEO Mr. Moneypocket

Cybersecurity Department Allocation

BLUF: My recommendation is to locate the cybersecurity department to the executive department level for appropriate risk management placement, IT department independence, and formal executive level oversight.

Executive Level of Oversight

As of 2026, cyber risks are one of the most prevailing and devastating types of damage that can occur to a company. Cybercrime is only becoming more sophisticated and vulnerability exploitation is a serious risk. For this reason, it must be taken under direct oversight and management of the executive department. Our CISO will provide guidance and direct reports to you and the board, and risk management focus will be elevated to enterprise level. Do note that we will need clearly defined boundaries established to prevent redundancy of responsibilities. Cybersecurity technical depth may needed to be handled with care when reporting to ensure the reports are understood.

Independence from IT

With the growth of cybercrime and with-it cybersecurity, it has reached a point of critical mass. Meaning it now has too large of a significance to be a subdepartment in IT. With the two departments separated, audits will be conducted without bloat slowing the process down.

Backlog issues can be avoided, and CISO's responsibilities can be performed with less interruption from IT jurisdictions and protocols. With the two separate however, there may be issues with required coordination. Cybersecurity will still rely on IT for implementation, access in infrastructure, and problem solving actions.

Risk Management Priority

Cybersecurity has now become a fundamentally enterprise risk function and should be positioned accordingly within the organization. Placing cybersecurity at the executive level aligns it with broader risk governance frameworks, including enterprise risk management (ERM). This placement ensures that cyber risk is evaluated alongside financial, operational, and reputational risks. This focused attention will demonstrate to shareholders and board members that the company's success is safeguarded by policy that is taking itself seriously. Possible concerns may relate to striking a balance between reporting and execution data over operational execution.

Conclusion: Positioning the cybersecurity department at the executive level sets an appropriate baseline standard. Independence from IT level bureaucracy, strengthened executive level accountability, and elevated cyber risk priority are just a few of the advantages. A direct reporting structure to executive leadership and the Board establishes clear authority, transparent escalation pathways, and disciplined risk management. This structure best protects the organization's long-term stability, compliance posture, and strategic objectives.