

Twaitney Addison

2/9/2026

CYSE200T

Professor: Duvall

AI Assignment

## **MEMO**

To: Chief Executive Officer

From: Twaitney Addison

Subject: Placement of the Cybersecurity Department

Date: 2/9/26

### **BLUF:**

The cybersecurity department should report directly to the CEO to ensure independence, strategic visibility, and effective management.

### **PURPOSE:**

The purpose of this memo is to recommend where the company's cybersecurity department should be located within the organization to best manage risk, meet regulatory expectations, and support long-term business objectives.

### **ANALYSIS:**

Cybersecurity is no longer a technical issue. Cyber incidents can disrupt operations, result in regulatory penalties, cause financial loss, and damage corporate reputation. As a publicly traded company, these risks directly impact shareholder value and executive accountability.

Placing cybersecurity under IT provides strong technical alignment but risks conflicts between speed and security. Placement under finance strengthens governance but may reduce operational responsiveness. Placement under operations supports continuity but can deprioritize long term risk oversight.

Reporting directly to the CEO ensures cybersecurity operates independently of competing departmental priorities and that cyber risk is evaluated alongside financial, legal, and operational risks. This structure improves executive awareness and aligns with modern regulatory expectations.

#### PROs:

- Elevates cybersecurity to a strategic business function
- Improves executive visibility and accountability
- Aligns with regulatory and shareholder expectations
- Enables faster executive level decision making during incidents

#### CONs

- Higher costs due to a standalone department
- Requires strong cross department coordination
- Depends on effective delegation from the CEO

These challenges can be mitigated through formal governance processes and strong collaboration with IT, finance and Operations.

#### CONCLUSION:

Given the company's public status and exposure to evolving cyber threats, locating the cybersecurity department under direct CEO oversight provides the best balance of authority, independence, and strategic alignment. This placement positions cybersecurity as a core component of enterprise risk management and supports the company's long-term resilience and shareholder trust.

# AI response

## Locating a Cybersecurity Department in a Large Publicly Traded Company

### Introduction

As cyber threats continue to increase in frequency, sophistication, and potential business impact, establishing a formal cybersecurity department has become a strategic necessity for large publicly traded companies. Beyond defining its technical responsibilities, an equally important decision is determining where this new department should reside within the organizational structure. The reporting line of cybersecurity significantly influences its authority, effectiveness, independence, and alignment with business objectives.

Common proposals place cybersecurity under Information Technology (IT), Finance, Operations, or directly under the Chief Executive Officer (CEO). Each option offers distinct advantages and drawbacks related to governance, risk management, compliance, cost control, and organizational influence. This analysis examines the pros and cons of each placement to support an informed decision.

**[Comment] What makes cybersecurity an enterprise-wide risk instead of something IT alone should handle?**

## Cybersecurity Under the Information Technology Department

### Pros

Placing cybersecurity within the IT department is the most traditional and commonly adopted approach. Cybersecurity teams often rely on IT infrastructure, tools, and personnel, making operational coordination straightforward. Shared technical knowledge allows for faster incident response, streamlined system integration, and efficient implementation of security controls.

This structure can also reduce costs by leveraging existing IT resources, avoiding duplicated tools or staff. For organizations in the early stages of cybersecurity maturity, IT oversight may provide a practical and familiar foundation.

### Cons

The primary concern with this model is a lack of independence. IT departments are often evaluated on system availability, performance, and speed of deployment, while cybersecurity prioritizes risk reduction and control. These goals can conflict, potentially leading to security compromises in favor of operational convenience.

Additionally, cybersecurity risks extend beyond technology into legal, financial, and reputational domains. When cybersecurity is treated purely as a technical function, enterprise-wide risk visibility may be limited, and security concerns may not receive adequate executive attention.

# Cybersecurity Under the Finance Department

## Pros

Locating cybersecurity within Finance emphasizes its role in enterprise risk management, regulatory compliance, and protection of shareholder value. Finance departments are deeply involved in risk assessment, audits, internal controls, and regulatory reporting—areas closely aligned with cybersecurity governance.

This structure can strengthen oversight, improve budgeting discipline, and elevate cybersecurity discussions to a business-risk level rather than a purely technical one. It may also enhance alignment with frameworks such as SOX, SEC cybersecurity disclosure requirements, and insurance considerations.

## Cons

Finance departments typically lack deep technical expertise, which can slow decision-making or result in over-reliance on IT or external consultants. Day-to-day operational security tasks, such as monitoring threats or responding to incidents, may suffer if the department is too far removed from technical teams.

There is also a risk that cybersecurity investments are viewed primarily as cost centers rather than strategic enablers, potentially limiting innovation or proactive security initiatives.

**[Comment] How could placing cybersecurity under Finance slow down technical response during an attack?**

## Cybersecurity Under Operations

### Pros

Placing cybersecurity under Operations highlights its role in ensuring business continuity, system reliability, and resilience. This structure aligns cybersecurity closely with manufacturing, logistics, service delivery, and operational technology (OT) environments, which are increasingly targeted by cyber threats.

For organizations with critical infrastructure or complex supply chains, this model can improve coordination between security and operational teams, reducing downtime and improving incident recovery.

### Cons

Operations departments are often focused on efficiency, throughput, and cost reduction. As with IT, these priorities can conflict with cybersecurity controls that introduce friction or slow processes.

Additionally, Operations-led cybersecurity may underemphasize strategic risk management, regulatory compliance, and long-term governance, especially in organizations with significant data privacy or financial reporting obligations.

## Cybersecurity Reporting Directly to the CEO

### Pros

Having cybersecurity report directly to the CEO elevates it to a strategic, enterprise-wide function. This structure provides independence from competing departmental priorities and ensures direct visibility at the highest level of leadership.

It reinforces cybersecurity as a business risk equal to financial, legal, and operational risks, supporting stronger governance and faster executive decision-making during incidents. This

model is increasingly favored by regulators and best-practice frameworks, especially for publicly traded companies facing disclosure and fiduciary obligations.

## Cons

Direct reporting to the CEO may be challenging to sustain operationally. CEOs often lack the time or technical background to oversee detailed cybersecurity activities, requiring strong delegation and clear governance processes.

This structure may also increase costs, as cybersecurity becomes a standalone function requiring its own administrative and support resources. Without careful integration, coordination with IT and Operations can become more complex.

## Conclusion

There is no single universally correct placement for a cybersecurity department; the optimal choice depends on organizational size, industry, risk profile, and cybersecurity maturity. Housing cybersecurity under IT offers technical efficiency but risks reduced independence. Placement under Finance strengthens governance and risk oversight but may weaken operational responsiveness. Operations alignment supports resilience and continuity but can downplay strategic risk. Reporting directly to the CEO provides the strongest authority and visibility, though it requires mature leadership structures to function effectively.

For large publicly traded companies facing regulatory scrutiny and significant cyber risk, many organizations adopt a hybrid model: cybersecurity leadership (such as a Chief Information Security Officer) reports to the CEO or a risk-focused executive, while maintaining strong dotted-line collaboration with IT, Finance, and Operations. This approach balances independence, technical effectiveness, and enterprise alignment, positioning cybersecurity as both a protective and strategic business function.