The Prompt:

I am part of a large publicly traded company. We are starting a cybersecurity program and debating where this new department should be located in the organization. Some say it should be under the information technology department, while others say it should be under Finance. Still others think it should be under Operations. There are even those who think it should report directly to the CEO. Create a 2 – 4 page analysis of the pros and cons of locating our new Cybersecurity department in these areas of the organization.

ChatGPT Output:

Cybersecurity Under the Information Technology Department
Pros

- Natural Alignment: IT manages infrastructure, networks, and systems—the same assets cybersecurity protects.
- Operational Synergy: Close collaboration with IT enables faster response to incidents and efficient integration of security controls into existing technology projects.
- Technical Expertise: IT teams often already include professionals with security-related knowledge, making the transition smoother.

Commented [HA1]: I wonder about training resources? If any, what are necessary skills needed?

Cons

- Potential Conflicts of Interest: IT may prioritize uptime, cost, and convenience over security, leading to tension or deprioritization of security needs.
- Perception as "Just IT": Cybersecurity risks may be viewed as purely technical issues, when they also involve business, regulatory, and reputational risks.
- Limited Visibility: IT-focused reporting can limit senior leadership's awareness of broader enterprise risk exposure.

Commented [HA2]: Why should cost overbalance security needs in this department?

Commented [HA3]: Cost should be a bigger deal under the finance department.

Cybersecurity Under Finance
Pros

- Risk and Compliance Orientation: Finance is closely tied to risk management, internal controls, and regulatory compliance, all of which overlap with cybersecurity objectives.
- Executive Credibility: Finance departments often hold strong influence with senior executives and boards, ensuring cybersecurity gets attention at the highest levels.
- Data Protection Alignment: Since financial data is among the company's most sensitive assets, locating cybersecurity within Finance highlights its role in safeguarding critical information.

Commented [HA4]: How will this department balance the security measure with the potential impacts on budgeting though without heavily focusing on one?

Cons

- Limited Technical Expertise: Finance lacks the operational and technical expertise necessary for daily cybersecurity operations.
- Possible Disconnect: Placing cybersecurity under Finance could distance the function from IT, slowing down implementation of technical safeguards.
- Narrow Risk Lens: Finance may focus heavily on compliance and monetary exposure while overlooking operational or reputational risks.

Commented [HA5]: This seems very valid under this department.

Cybersecurity Under Operations
Pros

- Business Integration: Operations ensures day-to-day business continuity. Aligning cybersecurity here emphasizes security as a core business enabler.

Commented [HA6]: How would the operations make for a stable and strong cyber department? Tactics?

- Cross-Functional Reach: Operations typically interacts across multiple departments, offering broader visibility into how cybersecurity affects business processes.
- Focus on Resilience: Cybersecurity can be tied directly to disaster recovery, continuity of operations, and resilience planning.

Cons

- Diluted Focus: Operations leaders often prioritize efficiency and cost reduction, which could reduce attention to evolving security threats.
- Resource Competition: Cybersecurity may compete with other pressing operational needs, leading to underinvestment.
- Less Technical Orientation: Without strong technical expertise, Operations may struggle to manage the complexities of modern cyber threats.

Cybersecurity Reporting Directly to the CEO

Pros

- Strategic Visibility: Cybersecurity is elevated to an enterprise-level risk, ensuring consistent attention from the CEO and Board.
- Neutral Alignment: Reporting outside IT, Finance, or Operations avoids conflicts of interest and ensures balanced oversight.
- Cross-Department Authority: Direct reporting gives cybersecurity leverage to work across silos and influence company-wide decision-making.

Cons

- CEO Bandwidth: The CEO may lack time or technical expertise to directly manage a cybersecurity program day-to-day.
- Operational Disconnect: Without a close tie to IT or Operations, practical implementation may be slower.
- Resource Dependence: Budgeting and staffing could still require negotiation with other departments, complicating execution.

Commented [HA7]: The CEO does have many major focuses and may not be able to manage this?

09/7/2025

Ally Howard

Subject: Implementing a New Cybersecurity Program in IT Department

The cybersecurity program should side in the IT department because they hold strong technical knowledge of many systems, enabling them to respond quickly to threats as well as strong and smooth security measures across the department.

Placing a cybersecurity program in an IT department has many advantages. Any IT department holds a deep understanding of an organization's technological structure like systems and networks. These advantages allow this program to manage many different measures of security and respond rapidly to threats. Key components of an effective program consist of strong training, data protection, security policies, and even plans for incident responses.

IT departments have previously developed many relationships with other technology connections making it more accessible to different resources and support. Some cons of this program falling into this department could include an exaggeration of specific technology which could be a conflict with the IT department being responsible for the systems and non-technology securities too.

Overall, the cybersecurity program needs to cover all the bases like knowing risks ahead of time, good training, plans for emergency responses, protecting the departments network and many more. These factors will significantly increase their effectiveness and strength against certain threats and safely protect their department and program as a whole.