To: Boss

From: Benjamin Owusu

Date: 8/7/2025

Subject: Why Cybersecurity and the IT department should be placed together

Why the IT and Cybersecurity department?

Dear Boss,

I am writing to inform you that it would be best to have the cybersecurity department in the IT department. The bullet points below are from the research I've conducted on the Benefits and Cons of having the Cybersecurity Department within the IT department.

Benefits

- Putting both IT and Cybersecurity departments together will guarantee faster coordination in dealing with cyberattacks due to a larger number of tech teams ready to prevent these attacks from happening in the company.

- IT professionals have a great understanding of the major vulnerabilities while storing information, such as Malware attacks, Data leaks, and breaches. This will enable both departments to use their skills and tools available to deal faster with upcoming attacks in the future.

- Ensures that IT operations, such as helping employees with computer problems, maintaining company wifi and vpn servers, and installing applications on work computers, are done safely without revealing sensitive information to hackers and other individuals outside the company

Cons

- Both the Cybersecurity and IT Departments might experience conflict over budgeting for resources that are being used, such as Separate Internet servers, IDS/IPS systems, and Firewalls.

- Cybersecurity protocols, such as resetting passwords at a certain time for each application used on company computers, will take time for the IT department to complete their day-to-day protocols, such as maintaining wifi servers and making sure computer applications are running smoothly.

Conclusion:

With the benefits presented, I believe that future cyber threats in the future will be dealt with quicker due to larger amounts of people working to resolve cyber attacks against the company, along with the cons presented. I believe that with the right amount of budgeting to overcome conflict between the two departments is possible.

AI Analysis USED BY Perplexity:

Locating the new Cybersecurity department within a large publicly traded company requires careful consideration of multiple organizational models. Each placement—under IT, Finance, Operations, or reporting directly to the CEO—offers distinct advantages and potential drawbacks for alignment, effectiveness, and risk management. Below is a detailed analysis of each option.

Under Information Technology (IT)

The traditional and most common structure is placing Cybersecurity within the IT department.

Pros

- Technical integration: Cybersecurity directly affects network management, software, hardware, and infrastructure. Placing it under IT ensures seamless coordination with existing technical teams and faster response to threats.
- Resource synergy: IT professionals understand systems architecture, data flows, and vulnerabilities, allowing effective use of skills and tools.
- Operational efficiency: IT-led security operations often enable streamlined incident management and system updates.

Cons

- Limited business perspective: Prioritization can become skewed toward technology projects rather than organization-wide risk management or business continuity.
- Potential conflict of interest: IT's operational goals (uptime, innovation, cost control) may at times conflict with security priorities (access control, compliance, risk reduction).
- Budget constraints: Cybersecurity might compete with other IT needs for resources, resulting in insufficient investment in security initiatives.

Under Finance

Some organizations place the Cybersecurity function under Finance, especially when focusing on risk and regulatory compliance.

Pros

- Risk alignment: Finance departments have a strong orientation toward risk management and compliance, aligning cybersecurity programs with regulatory requirements and financial controls.
- Budgetary control: Direct oversight by finance can result in better alignment with enterprise strategy and cost management, preventing wasteful spending and focusing on outcomes.
- Focus on business impact: Financial teams are adept at evaluating the business risk of cyber threats, and can drive stronger links between security investments and protection against potential financial losses.

Cons

- Knowledge gap: Finance leaders may lack technical expertise to assess, prioritize, or manage cybersecurity threats effectively, potentially undervaluing needs or misallocating resources.
- Operational disconnect: Finance-driven cybersecurity teams may not respond as quickly or understand operational needs as well as technical staff.
- Compliance focus: The department may emphasize compliance over proactive threat mitigation, treating cybersecurity as an audit function rather than a critical risk.

Under Operations

Embedding Cybersecurity within Operations centers the program around business continuity, process reliability, and service delivery.

Pros

- Business continuity: Operations teams focus on organizational processes and continuity, making them attentive to operational impacts of cyber incidents.
- Holistic risk management: Security becomes part of the broader operational risk management framework, which may improve resilience and cross-functional collaboration.
- Incident preparedness: Operations-driven models often prioritize incident response and recovery, key areas for minimizing business disruption.

Cons

- Diffuse responsibility: Cybersecurity may not receive the necessary focus or resourcing given the breadth of operational concerns, diluting ownership and expertise.
- Lack of specialized knowledge: Operations leaders might not possess sufficient understanding of complex threat landscapes, resulting in an overly generic or reactive security posture.
- Misaligned priorities: Operational objectives (efficiency, reliability) occasionally conflict with security best practices (access management, change control), potentially creating tension.

Reporting Directly to the CEO

Increasingly, organizations advocate for a direct line from the Cybersecurity leader (often the CISO) to the CEO to elevate security's strategic importance.

Pros

- Visibility and influence: Direct reporting ensures cybersecurity has the Board's attention and priority, enhancing resource allocation and strategic integration.
- Enterprise-wide perspective: Fosters cross-departmental cooperation and alignment with organizational goals, avoiding the "silo effect" of departmental placement.
- Balanced risk management: The CEO can broker effective trade-offs between business goals and risk, while the CISO advocates for robust defenses.

Cons

- Potential lack of technical oversight: CEOs may lack hands-on knowledge of cyber threats, leading to gaps in technical understanding or delayed decision-making.
- Competing priorities: CEOs must balance numerous urgent issues; cybersecurity may receive less dedicated time or focus than required, risking oversight gaps.
- Organizational tension: Direct reporting can disrupt existing structures and cause friction among peers, particularly IT and Operations leaders.

Comparison Table

Option	**Key Pros**	**Key Cons**
IT	Integration, technical expertise, efficient operation	Risk of neglecting business priorities, budget conflict

Finance	Risk alignment, budget control, compliance	Knowledge gap, slow response, compliance over security
Operations	Continuity, incident management, holistic approach	Diffuse focus, generic posture, priority tension
CEO	Visibility, influence, cross-functional cooperation	Limited technical knowledge, competing priorities

---

Conclusion

For large publicly traded companies, the ideal reporting structure for Cybersecurity depends on organizational priorities, leadership culture, and risk appetite. Many experts recommend a hybrid approach: empowering the CISO with direct access to the CEO and Board, but ensuring close collaboration with IT, Finance, and Operations for synergy and resilience. This structure best positions cybersecurity as a core business risk, not merely a technical concern.