Seth Sarauw
CYSE 200T
September 18, 2025
Professor Duvall

Organizational Placement of the Cybersecurity Department: Analysis of Options

Introduction

As a large publicly traded company, our cybersecurity posture is critical not only to operational resilience but also to shareholder confidence, regulatory compliance, and long-term strategic growth. Establishing a dedicated cybersecurity department is a positive step, but a key decision remains: where should the department be positioned within the organizational structure?

Several options are under consideration: locating cybersecurity under **Information Technology (IT)**, **Finance**, **Operations**, or reporting directly to the **Chief Executive Officer (CEO)**. Each structure has implications for governance, independence, influence, and resource allocation. This analysis explores the advantages and disadvantages of each approach.

Commented [1]: I find it very fascinating that it is referring to the CSF 2.0 sixth function added to this update. I wonder how it knew I wanted it to be up to date with CSF 2.0. Is it maybe to this with the last prompt we had to do comparing CSF 1.1 and CSF 2.0?

Option 1: Cybersecurity Under Information Technology

Pros

- **Technical Alignment**: Cybersecurity shares infrastructure, systems, and resources with IT, making collaboration efficient.
- **Operational Synergy**: Both functions manage networks, data, and systems, reducing duplication of effort.
- **Familiar Reporting Lines**: Many organizations already place cybersecurity under IT, providing a familiar and straightforward model.

Commented [2]: What does this mean when they say "reducing duplication of effort"?

Cons

- **Potential Conflicts of Interest**: IT is responsible for implementing systems, while cybersecurity is tasked with identifying weaknesses. Reporting within IT can compromise independence.

- **Risk of Prioritization Gaps**: IT often emphasizes uptime, efficiency, and innovation, which may conflict with cybersecurity's focus on risk reduction.

- **Limited Strategic Visibility**: Cybersecurity issues may be seen as "technical problems" rather than enterprise-wide business risks.

Commented [3]: Could we compare this with the 3 branches in the government (Judicial, Executive, and Legislative) and how they need to be separate and one can't be more powerful than the other?

Option 2: Cybersecurity Under Finance

Pros

- **Regulatory and Compliance Alignment**: Finance already oversees financial reporting, audits, and compliance with laws such as SOX. Cybersecurity reporting into Finance can strengthen risk management and regulatory oversight.

- **Investor Confidence**: Placing cybersecurity under Finance highlights the company's commitment to protecting shareholder value.

- **Risk Management Focus**: Finance functions often emphasize risk control, aligning well with cybersecurity's goals.

Commented [4]: What is SOX exactly?

Cons

- **Limited Technical Expertise**: Finance leaders may not have deep technical backgrounds, leading to gaps in understanding operational needs.

- **Disconnect from IT and Operations**: Cybersecurity threats often require immediate coordination with IT and Operations; Finance may be less agile in incident response.

- **Perception as Compliance-Only**: Cybersecurity risks may be narrowly framed as financial or audit concerns, overlooking broader operational threats.

Option 3: Cybersecurity Under Operations

Pros

- **Integration with Core Business Functions**: Operations ensure daily business continuity, and cybersecurity is increasingly tied to maintaining that continuity.
- **Focus on Business Impact**: Cybersecurity risks would be evaluated in terms of operational disruption and customer impact.
- **Stronger Incident Response**: Operational leadership may be better positioned to coordinate cross-departmental responses.

Cons

- **Less Emphasis on Compliance**: While Operations excels at continuity, it may not prioritize regulatory and financial reporting requirements as strongly.
- **Resource Competition**: Cybersecurity could compete with other operational priorities, potentially diluting its focus.
- **Risk of Being Seen as a Support Function**: Operations departments sometimes view cybersecurity as overhead rather than a strategic necessity.

Option 4: Cybersecurity Reporting Directly to the CEO

Pros

- **Strategic Visibility**: Reporting to the CEO elevates cybersecurity to a board-level and enterprise-wide priority.
- **Independence and Objectivity**: Avoids conflicts of interest by not being embedded within IT, Finance, or Operations.
- **Cross-Functional Authority**: Enables the cybersecurity department to influence policies and practices across all business units.

- **Shareholder and Market Confidence**: Demonstrates a clear commitment to protecting digital assets and customer trust.

Cons

- **CEO Bandwidth**: The CEO has broad responsibilities, and day-to-day oversight of cybersecurity may be impractical.
- **Risk of Isolation**: Without careful integration, the cybersecurity department could become siloed, disconnected from technical and operational functions.
- **Resource Allocation**: May require the creation of new governance structures (e.g., a Chief Information Security Officer with board visibility).

Conclusion and Recommendation

Each reporting structure has clear strengths and limitations. Placement under IT ensures technical alignment but risks independence. Finance emphasizes compliance but may lack agility. Operations integrates cybersecurity with continuity but may undervalue regulatory priorities. Direct reporting to the CEO elevates cybersecurity strategically but requires careful governance design.

Best practice among large publicly traded companies is increasingly to establish cybersecurity as a function led by a Chief Information Security Officer (CISO), reporting either directly to the CEO or jointly to the CEO and the Board's Audit or Risk Committee. This approach balances independence, visibility, and authority while ensuring strong cross-departmental coordination.

Given the high regulatory scrutiny, shareholder expectations, and reputational risks faced by our company, we should adopt a **CEO-level reporting structure**, supported by strong dotted-line relationships with IT, Finance, and Operations. This ensures cybersecurity is treated not merely as a technical or compliance matter, but as a strategic business priority.