ASSIGNMENT

Student Name
Oluwatimilehin Oluwagbemi

Reg. No
2025/GRC/10712

7th Spetember, 2025

Course Title
GRC 101 – Information Security Governance

Introduction

This assignment focused on a thorough examination of security governance using organizational data and actual incidents. It begins by looking at how the Chief Information Security Officer's (CISO) role has changed over time, emphasizing on the move from technical supervision to strategic leadership. Uber's breach concealment case was used to highlight the negative effects of executive-level unethical behavior and lack of oversight.

Colonial Pipeline ransomware attack which reveals governance flaws such as outdated infrastructure, loose access controls, and low board participation is the case study addressed. When these observations are applied to incident data from NDPC, a multinational IT company, it is evident that the risks are similar. The NDPC dataset analysis reveals three key governance gaps: the high cost of severe incidents, inconsistent departmental performance, and incomplete incident closure.

The assignment concludes with practical suggestions for NDPC, such as improved board-level cybersecurity oversight, SLA-based incident tracking, and infrastructure modernization. These tactics are based on industry best practices and conform to international standards like ISO/IEC 27001 and NIST.

The Evolving Role of the Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) now plays a strategic, board-level leadership role, having changed from a largely technical one over the last ten years. CISOs were traditionally responsible for overseeing technical compliance, managing firewalls, and keeping an eye on threats. However, CISOs are now expected to function as business enablers, striking a balance between security requirements and organizational growth objectives, as the threat landscape has become more complex and regulatory scrutiny has increased.

Shift in Responsibilities:

- In the past, CISOs concentrated only on technical configurations, perimeter/firewall defense, and IT security controls.
- Currently, CISOs are directly responsible for security governance and resilience, supervise enterprise-wide risk management, and guarantee adherence to international laws (such as GDPR, HIPAA, and PCI DSS). In order for executives and boards to make well-informed risk-based decisions, they must convey security priorities in business terms (Gartner, 2024).

Shift in Reporting Structure:

- In the past, CISOs frequently answered to the CIO, which posed the risk of presenting security as an IT subset.

- The strategic significance of cybersecurity governance is highlighted by the fact that many organizations today have reorganized so that CISOs report directly to the CEO or the board of directors.

Real-World Example:
The Equifax data breach that occurred between May and July 2017, resulting in the compromise of personal information of over 147 million people, is a notable example. To address the issue Equifax released a statement announcing the departure and replacements of its chief information officer and chief security officer elevated to report directly to the board. This modification demonstrated how insufficient executive-level visibility had previously hampered efficient governance (Wikipedia).

Case Study: Colonial Pipeline Ransomware Attack (2021)

Overview of the Breach:
On the 7th of May, 2021, Colonial Pipeline, an American oil pipeline system that originated from Houston Ttexas suffered a ransomware cyberattack that affected computer equipment managing the pipeline. The Colonial Pipeline had to temporarily stop operations to contain the attack. The attackers gained access to the system using a compromised password for an inactive virtual private network (VPN) account, which did not have multi-factor authentication enabled (Wikipedia).

Security Governance Structure Prior to the Breach:
Publicly available reports suggest that Colonial Pipeline may have lacked robust cybersecurity governance practices in two critical areas: incident response planning and access management. There were governance flaws in the way executive leadership prioritized cybersecurity over operational resilience, even with security teams in place.

Failures in Security Governance:

- **Weak Identity Management:** Absence of multi-factor authentication on critical accounts.
- **Board Oversight Gaps:** Cyber risks were not adequately escalated to the board level.
- **Incident Preparedness:** Although the company had some security policies, there was no evidence of a mature, enterprise-wide governance framework to guide incident response (NIST, 2018).

Regulatory and Financial Consequences:
The Colonial Pipeline had to pay a sum of $4.4 million as ransom overseen by the FBI (Wikipedia). Apart from the immediate costs, the hack resulted in increased regulatory scrutiny, and US federal agencies required pipeline operators to adhere to more stringent cybersecurity guidelines. According to Shackelford reputational damage doesn't only damage public trust but also exposes governance shortcomings in the protection of critical infrastructure (Shackelford, 2020).

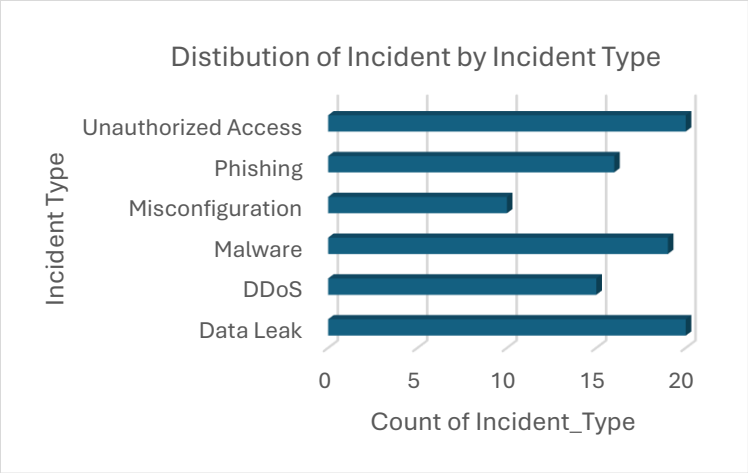
Recommendations for Improved Governance:

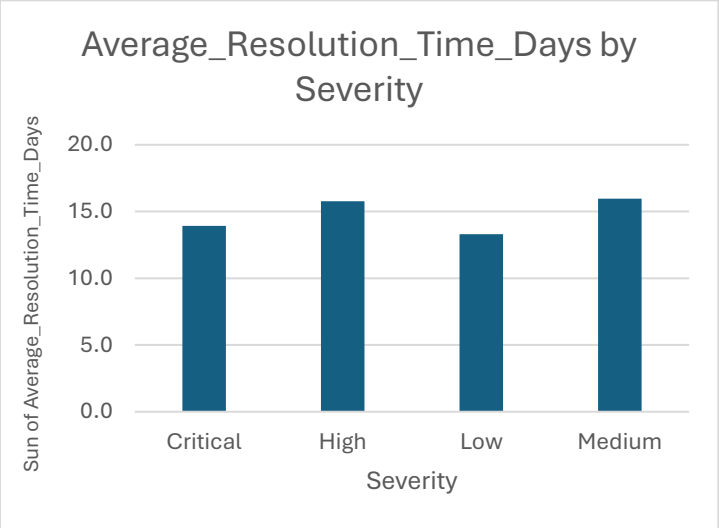
- Implement **strong** access controls with mandatory multi-factor authentication.
- Develop a comprehensive incident response framework aligned with NIST Cybersecurity Framework (CSF) (NIST, 2018).
- Elevate the CISO's role to ensure direct communication with the board, enabling proactive risk management.
- Conduct regular governance-focused cybersecurity audits to validate readiness against ransomware and other critical threats.

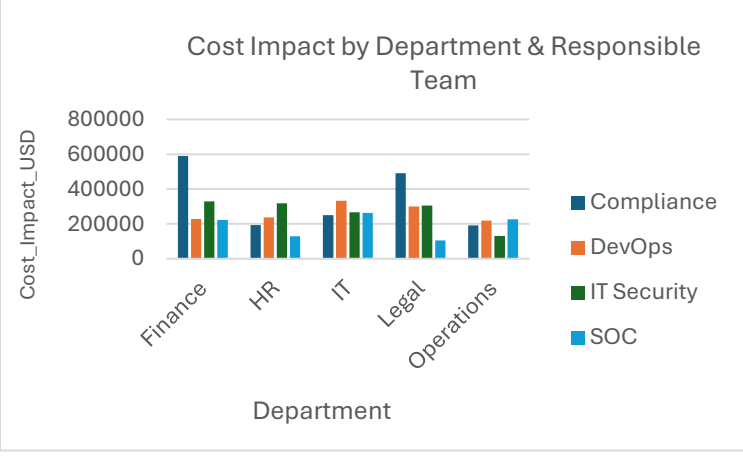
NDPC Case Study

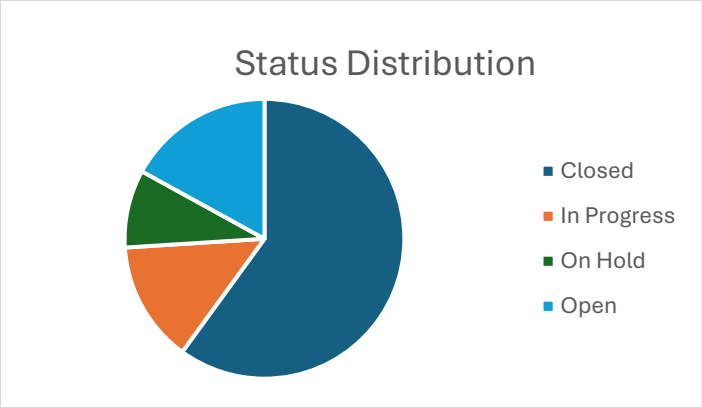
Data Analysis:

- The total number of Incident is 100:
  - 20 Unauthorized Access Incidents,
  - 20 Data Leak Incidents,
  - 19 Malware Incidents,
  - 16 Phishing Incidents,
  - 15 DDoS Incidents and
  - 10 Misconfiguration Incidents.
- Average Resolution_Time_Days broken down by severity:
  - 13.9 Critical Severity
  - 15.8 High Severity
  - 16.0 Medium
  - 13.3 Low
- Total Cost Impact by Department and Responsible Team
  - Finance Department has the highest cost of $1.37M, followed by Legal Department with cost of $1.2M, and IT with cost of $1.1M. HR and Operations has the least cost Impact of $879K and $767K.
  - Compliance team has the highest cost impact.
- The top 3 Incident type with the highest cost impact are; Malware, Misconfiguration and Unauthorized Access.
- Percentage of Incident with Status:
  - 60% Closed
  - 14% In Progress
  - 9% On Hold
  - 17% Open


Distibution of Incident by Incident Type
Incident Type
Unauthorized Access
Phishing
Misconfiguration
Malware
DDoS
Data Leak
0
5
10
15
20
Count of Incident_Type


Average_Resolution_Time_Days by Severity
Sun of Average_Resolution_Time_Days
20.0
15.0
10.0
5.0
0.0
Critical
High
Low
Medium
Severity


Cost Impact by Department & Responsible Team
Cost_Impact_USD
800000
600000
400000
200000
0
Finance
HR
IT
Legal
Operations
Department
Compliance
DevOps
IT Security
SOC



Insight 1: High Financial Impact Concentrated in Finance and Compliance

The cost analysis showed that the Finance department spent the most money overall ($1.37M) on incident-related expenses, followed by IT ($1.11M) and Legal ($1.20M). Similarly, the Compliance team outspent all other teams in charge by $1.72 million. These findings suggest that there are governance issues in departments that engage in sensitive, high-risk activities, which are also the areas with the greatest regulatory exposure.

Recommendation: In Finance and Compliance, NDPC should implement more robust preventive controls and carry out department-specific risk assessments. This entails regular compliance audits, improved access controls, and real-time process monitoring. In order to ensure board-level visibility and improve accountability, the CISO, Internal Audit, and Risk Management departments should share oversight of these high-risk departments (Shackelford, 2020).

Insight 2: Resolution Time Not Aligned with Severity

Unexpectedly, it took 16 days on average for incidents of Medium severity to be resolved, longer than even Critical incidents (13.9 days). This suggests that the prioritization of incident response is inconsistent. According to Cisco, there's a chance that unresolved incidents of medium and low severity won't get enough attention, which could lead to more serious breaches.

Recommendation: In accordance with guidelines like NIST CSF or ISO/IEC 27035, NDPC should to implement a risk-based prioritization framework (NIST, 2018). SLAs for incident response that ensure prompt resolution for all severities should be enforced by the CISO's office. Lower-severity incidents won't go unresolved for long thanks to the automation of triage and escalation procedures.

Insight 3: Governance Gaps in Incident Resolution Backlog

According to the analysis of incident status distribution, 31% of incidents are still Open or In Progress, meaning that even though 60% of incidents have been closed, a sizable portion are still unresolved. This backlog is a result of either insufficient governance oversight, unclear

responsibilities, or limited team capacity. Leaving such a high volume of unresolved cases exposes NDPC to prolonged security risks.

Recommendation: A governance dashboard should be put in place by NDPC in order to monitor incident closure rates and report past-due cases straight to executive leadership. To better manage incident loads, the SOC and IT Security teams might also need more capacity or more advanced training. In order to promote accountability, the CISO should also incorporate closure metrics into board-level reporting (Gartner, 2024).

Conclusion

As this assignment highlights, effective security governance is a technical and strategic function. An illustration of how the role has evolved from being exclusively IT-focused to becoming strategically significant and necessitating board-level involvement is the evolution of the CISO position. The Colonial Pipeline case highlights the need for strong frameworks and executive oversight by demonstrating how bad governance can result in national crises.

The NDPC case study also shows how data-driven analysis can reveal governance flaws in accountability, cost management, and incident resolution prioritization. NDPC can improve its resilience, lower its regulatory exposure, and harmonize its security governance with international best practices by implementing the suggestions made.
Organizations will ultimately be better equipped to handle an increasingly hostile cyber threat landscape and maintain long-term operational success if they integrate governance, risk management, and compliance into their culture.

References

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Wikipedia. *Colonial Pipeline Ransomware Attack 2021*. https://en.m.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

2017 Equifax data breach – Wikipedia

Gartner. (2024). *Reframing the CISO Role to Drive Business Enablement and Resilience*. Gartner Research. https://www.gartner.com/en/documents/5751415

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

Shackelford, S. J. (2020). Governing cybersecurity: Global responses to technological risks. *International Journal of Law and Information Technology*, *28*(2), 93–118. https://doi.org/10.1093/ijlit/eaaa002