Cybersecurity Reflection Write-Up

Author: James E. Newman

Certificate: Google Cybersecurity Professional Certification (in progress)

Focus: Cloud Security + Governance, Risk and Compliance (GRC)

Executive Summary

Cybersecurity is business risk management. Modern organizations depend on secure systems to protect revenue, reputation, and customer trust. Through the Foundations course I've learned how core security principles (like confidentiality, integrity, and availability) translate into day-to-day decisions—everything from access control to incident reporting. This reflection summarizes those principles and explains why I'm focusing my portfolio on Cloud Security and GRC.

Why Cybersecurity Matters to Businesses

Every company is a technology company now. Customer data, payment systems, and operations live on networks and in the cloud. A single weak control can lead to financial loss, legal exposure, operational downtime, and long-term brand damage. Good security isn't just "IT hygiene"—it's part of how the business competes and keeps promises to customers.

Security also supports compliance. Regulations and frameworks (PCI DSS, HIPAA, SOC 2, ISO 27001, etc.) exist because customers and partners expect verifiable controls. Clear policies, risk assessments, and audit-ready documentation turn security from a reactive scramble into a repeatable process the business can trust.

Lessons From Major Breaches

Capital One – 2019
In 2019, Capital One suffered a major breach when a misconfigured AWS S3 bucket and overly broad IAM permissions allowed an attacker to exploit a server-side request forgery (SSRF) vulnerability. The breach exposed more than 100 million credit applications, including Social Security numbers, bank account details, and other sensitive customer information. It was discovered after the attacker (Paige Thompson) publicly boasted about the exploit online, which led a security researcher to report it to the company. The fallout was severe: Capital One faced lawsuits, customer distrust, and an $80 million fine from regulators. This breach could have been avoided with stronger cloud configuration reviews, tighter IAM policies, and continuous monitoring.

Lesson:
This incident highlights the critical need for Cloud Security Analysts and Engineers, whose roles include monitoring permissions, reviewing cloud configurations, and enforcing secure identity practices to prevent these types of vulnerabilities from being exploited.

Microsoft Azure – ChaosDB Vulnerability (2021)
In 2021, researchers at Wiz discovered a critical vulnerability in Microsoft's Azure Cosmos DB service, later nicknamed ChaosDB. The flaw allowed attackers to gain full administrative access to thousands of customer databases hosted in the cloud. This exposure put highly sensitive information at risk for some of Microsoft's largest enterprise clients. The issue was identified by the Wiz research team during a routine security review and responsibly disclosed to Microsoft. In response, Microsoft quickly disabled the vulnerable feature, notified impacted customers, and reset security keys. While there were no known active exploits, the potential damage was enormous. This situation underscored that even cloud providers themselves can introduce vulnerabilities.

Lesson:
This breach highlights the importance of organizations having Cloud Security Architects and Analysts who understand the shared responsibility model. Even when the provider secures the infrastructure, customers must still monitor their own environments, rotate credentials, and validate cloud service configurations against known risks.

Target – 2013
In late 2013, Target experienced one of the most notorious retail breaches in history after attackers gained access to its network through a third-party HVAC vendor with weak credentials. Once inside, the attackers installed malware on Target's point-of-sale systems, ultimately stealing 40 million credit card numbers and the personal data of more than 70 million customers. The breach was first identified when external banks and law enforcement began investigating unusual fraud patterns linked back to Target cards, which prompted Target to confirm the compromise. The fallout was devastating: Target's CEO resigned, the company paid over $200 million in settlements and security upgrades, and its reputation took a significant hit.

Lesson:
This incident highlights the importance of GRC Analysts and Third-Party Risk Managers who evaluate vendor access, enforce stricter security controls, and ensure compliance with risk management standards. Strong governance and oversight of third-party vendors could have closed the door before attackers ever got in.

What I Learned in Foundations (Key Principles I'll Apply)

- **CIA Triad**
    - **Confidentiality** – only the right people/systems access data (encryption, access control).
    - **Integrity** – data is accurate and unaltered (hashing, input validation, change control).
    - **Availability** – systems are up when needed (backups, redundancy, DDoS protection).

Least Privilege & Need-to-Know
Every user/service should have the minimum access required. This reduces the blast radius when credentials are misused.

Defense in Depth
Stack multiple controls—network segmentation, firewalls, MFA, logging—so one failure doesn't equal total compromise.

Threats vs. Vulnerabilities vs. Risk

- ○ Threat = something that can cause harm (attacker, malware, natural event).
- ○ Vulnerability = a weakness (unpatched software, default creds).
- ○ Risk = the likelihood and impact of a threat exploiting a vulnerability.

Security Is a Lifecycle
Identify assets, assess risk, implement controls, monitor, respond, and improve. Documentation and repeatability matter.

Why I'm Focusing on Cloud Security & Governance Risk and Compliance

Cloud is where today's workloads live. I want to learn how identity, network controls, encryption, and logging work in cloud environments—and how to harden Linux workloads that run there. At the same time, I'm drawn to GRC because it connects security work to business outcomes: policies that people can follow, risk registers leaders can use to decide, and reports that prove controls are working.

This portfolio will reflect both sides:

- Hands-on Cloud Sec: network diagrams, VM hardening, vulnerability scans, and log/incident write-ups.
- GRC: a simple risk assessment, clear remediation notes, and professional reporting.

How I’ll Apply This (What’s Next)

- Build a small cloud Linux VM and document basic hardening steps.
- Run a vulnerability scan and write a short remediation report.
- Enable logging/alerting and produce a mock incident report.
- Automate one task (e.g., parsing failed SSH logins) with Python.
- Keep everything organized and written in business-friendly language.

Closing

The Foundations course gave me the language and mindset of security: protect data, reduce risk, and support the business. The projects in this portfolio are intentionally small and practical so each one proves a specific skill. As I progress through the certificate, I’ll keep connecting technical controls to measurable risk reduction—especially in the cloud—while documenting the work clearly enough for any stakeholder to understand.

Note: This reflection also serves as a personal reference point that I’ll continue revisiting as I grow in cybersecurity. It represents the foundation for the more technical projects that follow in this portfolio.