Capital One Cybersecurity Plan

ITC 6520: Network Protection and Cloud Security

2023 Fall Quarter: Term A

Instructor: Carmen Taglienti

Presented by Group 1 (Titiksha Ghosh, Mina Holie, Edgardo Montoya)

Northeastern University

Agenda

1. **Introduction: Capital One**
   - Cyber incident case facts & project purpose/objectives
2. **Cybersecurity Strategic Plan**
   - Our approach: NIST Cybersecurity Framework (CSF)
3. **Solution Architecture**
   - Thought & design processes of the diagram
4. **Amazon Web Services (AWS) Cloud Services**
   - Key services for security risk mitigation & incident response/recovery
5. **Our Journey & The Road Ahead**

Introduction: Capital One

Company Information

- Large US financial institution
- Customers from all over North America and UK
- Highly regulated under cybersecurity laws and regulations

2019 Cyber Incident

- Data breach incident in 2019
  - Vulnerability taken as advantage by a former AWS employee
  - Misconfiguration of the firewall in a web application stored in AWS

Lessons Learned from the 2019 Incident

- Management of sensitive data in the cloud
- Management of risks arising from third-party service providers

Introduction: Capital One

Project Purpose

- Establish better security practices from lessons learned
- Ensure confidentiality, integrity, and availability
- Balance controls and efficiency
- Align with NIST Cybersecurity Framework (NIST CSF)
- Implement a new cybersecurity strategic plan

Cybersecurity Objectives

To enhance and safeguard the organization's information assets and IT infrastructure by implementing robust cybersecurity measures, reducing vulnerabilities, and minimizing an adverse impact on the business.

Cybersecurity Strategic Plan

Our Approach: NIST CSF

- Use as guidance to enhance the security of systems and data
- Provide a structured approach to safeguard an organization’s information assets and effectively manage cybersecurity challenges
- Think of it as a five-step plan: understand what matters, keep them safe, look out for issues, fix them when risks arise, and recover when things go wrong

Scope of the Plan Framework

- 5 core functions: Identify, Protect, Detect, Respond, Recover
- 13 categories
- 31 subcategories

Cybersecurity Strategic Plan

Identify (ID) - Focus on asset understanding & risk management

Asset Management (AM)	**Governance (GV)**	**Risk Assessment (RA)**	**Risk Management Strategy (RM)**
ID.AM-5 Resources	**ID.GV-1** Organizational cybersecurity policy	**ID.RA-3** Threats identified & documented	**ID.RM-1** Risk management processes established, managed, & agreed by stakeholders
ID.AM-6 Cybersecurity roles & responsibilities	**ID.GV-2** Cybersecurity roles & responsibilities aligned with internal roles & external partners	**ID.RA-4** Potential business impacts & likelihood identified	**ID.RM-2** Risk tolerance determined & expressed
	ID.GV-3 Legal & regulatory requirements	**ID.RA-6** Risk response identified & prioritized	**ID.RM-3** Determination of risk tolerance informed

Cybersecurity Strategic Plan

Protect (PR) - Enhance measures to protect information assets

Identity Management & Access Control (AC)	**Awareness & Training (AT)**	**Data Security (DS)**	**Protective Technology (PT)**
PR.AC-1 Identities/Credentials managed & audited	**PR.AT-1** All users informed & trained	**PR.DS-1** Data-at-rest protected	**PR.PT-1** Log records implemented & reviewed
PR.AC-3 Remote access		**PR.DS-5** Protection for data leaks	**PR.PT-3** Least privilege
PR.AC-4 Permissions & authorization managed			**PR.PT-5** Mechanisms to achieve resilience requirements
PR.AC-5 Network integrity			
PR.AC-7 Devices authenticated			

Cybersecurity Strategic Plan

Detect (DE) - Enable timely detection of potential threats

Security Continuous Monitoring (CM)
DE.CM-1 Network monitored
DE.CM-4 Malicious code detected
DE.CM-8 Vulnerability scans performed

Cybersecurity Strategic Plan

Respond (RS) - Execute the incident response effectively

Response Planning (RP)	Mitigation (MI)
RS.RP-1 Response plan executed during or after an incident	**RS.MI-1** Incidents contained
	RS.MI-2 Incidents mitigated

Cybersecurity Strategic Plan

Recover (RC) - Carry out the disaster recovery effectively

Recovery Planning (RP)	Communications (CO)
RC.RP-1 Recovery plan executed	**RC.CO-1** Public relations managed
	RC.CO-3 Recovery activities communicated internally & externally

Solution Architecture

Capital One’s Security Environment

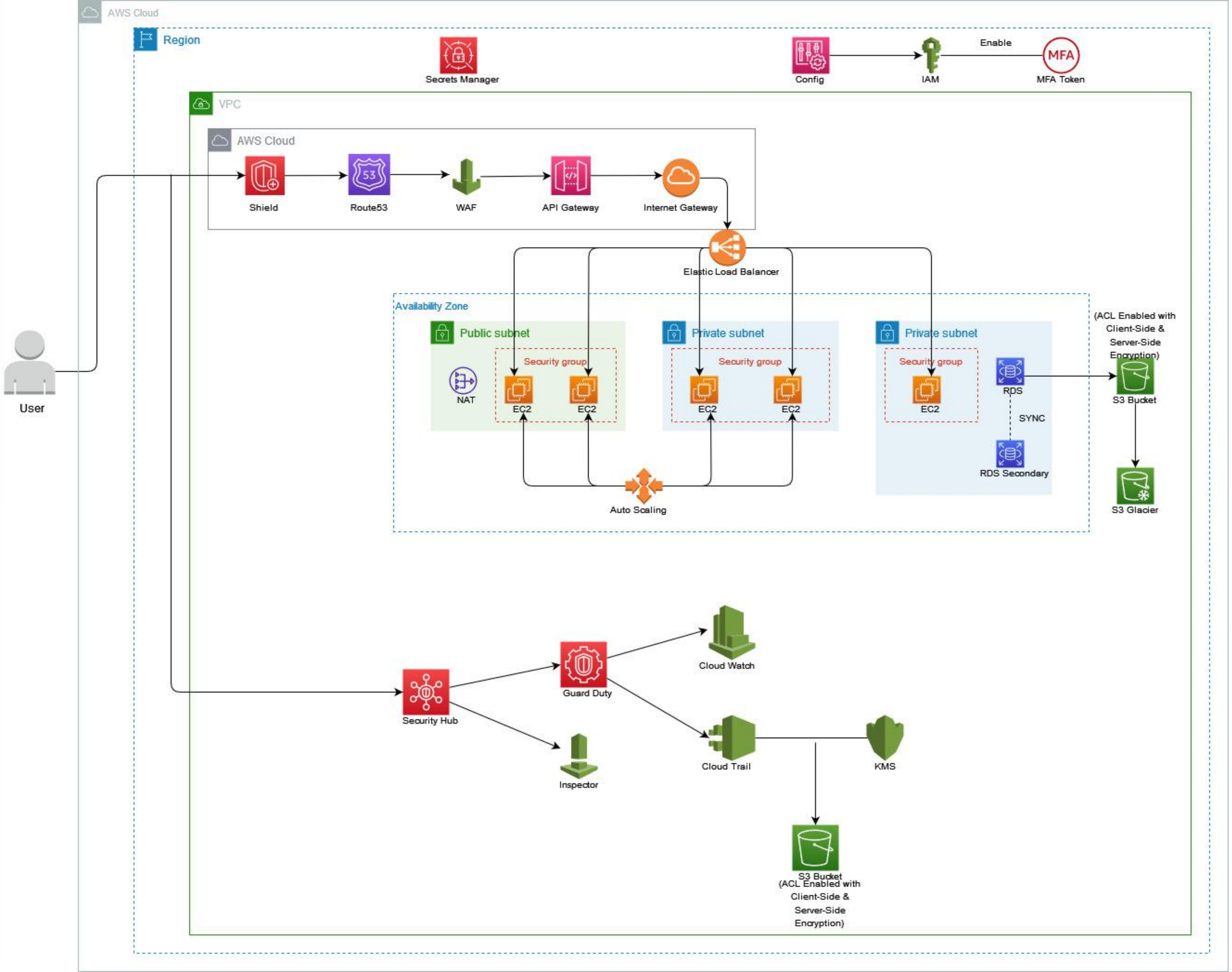
- At the time of the 2019 security incident
- Security holes identified
- Desirable security environment

Diagram: Our Architectural Approach

- Thought process
- Design process

Security Objectives

- What aspects of the system will be improved?
- What risks can be mitigated?


AWS Cloud
Region
Secrets Manager
Config
IAM
Enable
MFA
MFA Token
VPC
AWS Cloud
Shield
Route53
WAF
API Gateway
Internet Gateway
Elastic Load Balancer
User
Availability Zone
Public subnet
Security group
NAT
EC2
EC2
Private subnet
Security group
EC2
EC2
Private subnet
Security group
EC2
RDS
SYNC
RDS Secondary
(ACL Enabled with Client-Side & Server-Side Encryption)
S3 Bucket
S3 Glacier
Auto Scaling
Cloud Watch
Guard Duty
Security Hub
Inspector
Cloud Trail
KMS
S3 Bucket
(ACL Enabled with Client-Side & Server-Side Encryption)

AWS Cloud Services

- IAM (Identity and Access Management)
- Secrets Manager
- WAF (Web Application Firewall)
- AWS Inspector
- AWS Guard Duty
- KMS (Key Management Service)
- CloudTrail
- AWS Secret Manager
- Cloud VPC (Virtual Private Cloud)
- Trusted Advisor

House, T. (2023). Top 25 AWS Services List 2023 (All Services). AllCode. https://allcode.com/top-aws-services/

IAM

The 2019 breach was due to a misconfigured IAM role. With stricter IAM policies and regular audits, such vulnerabilities can be mitigated.

Benefits for Capital One:

- **Fine-grained access control** - Ensures only authorized personnel can access specific resources, preventing unauthorized data access like in 2019.
- **Multi-factor authentication** - Adds an extra layer of security, making it harder for attackers to gain access.
- **Temporary credentials** - Reduces the risk of long-term unauthorized access.

Issues Addressed:

- ***ID.AM-6:*** Cybersecurity roles and responsibilities
- ***PR.AC-1:*** Identities and credentials issued, managed, verified, revoked, and audited
- ***PR.AC-3:*** Remote access managed
- ***PR.AC-4:*** Access permissions and authorizations managed

AWS IAM

AWS (IAM) - Amazon Web Services, Inc.
https://aws.amazon.com/iam/

AWS Guard Duty

By detecting unusual activity or unauthorized access attempts in real-time, it can prevent potential breaches, ensuring that incidents like 2019 are not repeated.

Benefits for Capital One:

- **Unusual activity detection** - Identifies and alerts on unusual API calls or potentially unauthorized deployments, preventing breaches like in 2019.
- **Real-time monitoring** - Ensures immediate response to any threats, reducing potential damage.

Issues Addressed:

- ***DE.CM-1:*** Network monitored
- ***DE.CM-4:*** Malicious code detected

Venkatesh, L. (2022). AWS Security Layer [png] — https://medium.com/nerd-for-tech/aws-series-2-deep-dive-aws-security-layer-network-web-apps-a629f60631ef

Our Journey & The Road Ahead

Zmicierkavabata. (2017). Road way location. https://www.istockphoto.com/vector/winding-road-on-a-white-isolated-background-with-pin-pointers-gm691423398-127526455

What We've Learned:

- Importance of stringent access controls.
- Need for continuous monitoring and real-time threat detection.
- Regular audits and reviews are crucial.

Next Steps:

- Implement additional AWS tools for a layered security approach.
- Create a plan for training sessions for Capital One staff on the best security practices.
- We will implement a security risk assessment for the Capital One systems periodically.

End of the Presentation