MILESTONE 4

Capital One:

Cybersecurity Initiation, Asset and Risk Analysis and Security Policy

Arsalan Ahmed, Steve John, Vraj Mehta, Reece Taplin, and Sarah Tse

The University of Texas at Dallas

Contents

MILESTONE 1: SECURITY INITIATION 4
Executive Summary 4
Security Specific Issues and Expectations 5
Security Categorization and High-Level Security Requirements 6
Security Requirements 6
Laws, Regulations, and Standards 6
Control Spreadsheet 8
Countermeasures/Controls 8
MILESTONE 2: RISK ASSESSMENT 9
Asset Identification 9
Risk Matrix 10
Risk Assessment 11
Key Security Roles 12
Key Stakeholders 12
MILESTONE 3: SECURITY POLICY 13
Introduction 13
Security Requirements, Goals and Scope 13
2.1 Requirements 13
2.2 Goals 13
2.3 Scope 14
Information Classification Map for Capital One 14
Restricted Information 16
Confidential Information 16
Internal Information 16
Public Information 16
Risks and Risk Matrix 17
Policies 19
Internet: 19
System Usage: 19
Anti-Virus 20
Physical Security 20
Email Policy 21

Data Usage 22
Password Policy 22
Acceptable Use 23
Policy Compliance 23
Responsibilities 24
Team Meeting Minutes 25
Works Cited 26

MILESTONE 1: SECURITY INITIATION

Executive Summary

The selected company for this project is Capital One Financial Corporation. Ranked as the 7th largest commercial bank in the nation based on consolidated assets, Capital One has over 700 domestic branches and over 170 foreign branches in operation (Federal Reserve System, 2019). Canada and the United Kingdom are the two foreign countries that receive Capital One's financial products and services. Therefore, we must consider the governing legislation and policies that affect financial institutions such as Capital One in each of these 3 countries. The primary emphasis of Capital One's products and services is in the credit services industry. According to Reuters, the company's main operations can be segmented in to 3 categories: credit card, consumer banking, and commercial banking (2019). For this project, our focus will be on Capital One's web application, which encompasses credit card and consumer banking operations.

According to Capital One's 2018 annual report, the company was ranked as the nation's third largest issuer of Visa and Mastercard credit cards (Capital One Financial Corp., 2019). Capital One's web application serves as a key credit management solution for consumers. By using the web application, users can make online payments, view billing history, activate new cards, and know their credit score through the CreditWise feature (Capital One, 2019a). Furthermore, requests for additional credit cards can be processed through the web application.

The 2018 annual report breaks the consumer banking category down into activities such as "deposit gathering and lending" and "national deposit gathering and national auto lending" (Capital One Financial Corp., 2019, pg.5). The types of accounts available to individuals include certificate of deposit, money market, and IRA (Capital One, 2019b). These accounts can be managed extensively through the web application. Users can open new accounts, conduct automatic transfers, pay bills, and manage funds directly from their computers (2019b).

The rise of online banking and digital credit management solutions have streamlined the banking process for many. However, online banking tools such as Capital One's web application

are at risk for cyber-attacks. Assets such as consumer data must be blanketed by strong layers of security safeguards, and risk assessments must be thoroughly conducted. This project will explore the security aspect of Capital One's web application and reflect strategies for defending against a variety of threats.

Security Specific Issues and Expectations

As many are aware, Capital One was recently a victim of one of the biggest data-breach in the history for a financial institution. Based on the recent events, we believe it is important to address some of the specific issues that led to these events. Some key security issues that Capital One faces are AWS server misconfigurations, insider threat, poor third-party vendor assessment, mismanaged system access, misconfigured/ mistuned IDS sensors, and more. In the case of the Capital One breach, the attacker was able to exploit most if not all of the above-mentioned vulnerabilities one by one. Doing so, they were able to go from gaining access to a single server, to getting their hands on 100 million records of customer data (Krebs, 2019).

This data breach caused significant amount of monetary and reputation loss for the company. As a result, the organization now expects a certain standard of security surrounding the listed security vulnerabilities. The company security expectations to address the misconfigured AWS servers, initial entry method of the attacker, are that the AWS servers and other third-party servers undergo both company and 3rd party security test before any company data or services are hosted on them. In order to address the insider threat utilizing the mismanaged permissions and access, the company expects a new permission policy that mimics the 'least privilege policy', and a full audit of the current granted permissions to each and every employee group. This will stop the attacker from exploiting further system and gaining access to other resources even if an employee account is compromised because at some point the account's allowed access will hit a barrier. Furthermore, the company will be conducting a deeper security assessment of the third-party software and resource provider as a whole and will also conduct an assessment of the individual 3rd party staff on projects that pertain to Capital One services and data. A reputable background assessment firm will be sought out and contracted to perform these third-party checks. The threat detection and prevention systems in place currently failed to detect and respond in time to prevent the data

leak, indicating a visibility gap, misconfigured sensors, or failed security process. As such, the company security division is expected to audit the network infrastructure for visibility gap and determine if additional sensors or other vendor products are needed, identify misconfigured sensors and issue their respective fix, determine if a security policy or process was not followed and issue mandatory training for the responsible parties. The listed security issues and security expectation are gathered from recent data breach at Capital One. In future, the company should and will continue monitoring the status of these vulnerabilities, scan for new vulnerabilities present, issue appropriate remediations, and continue to put precedence on security.

Security Categorization and High-Level Security Requirements

Security Requirements

The web application enables users to perform online banking functions which can include a wide variety of actions such as depositing checks and moving money through a web-based application. Previously, with in-person banking, customers were required to show a government issued ID and sign with a matching signature. However, with the digitalization of banking in recent years, higher incidents of fraud and identity theft have been reported to the Office for Victims of Crime (2018). As a result, security requirements have also increased and have become more complex. Specifically, the Capital One online banking web application security requirements are provided below:

- The application should authenticate users by prompting users for account email and password.
- The application should encrypt all information during transportation.
- The application should hash/encrypt sensitive information in storage.
- The application should have a digital certificate.
- The application should not have any unnecessary ports open.
- The application should implement a web application firewall (WAF).
- Accepted Risks should be reviewed and reconsidered on an annual basis.
- The application should limit user to three login attempts before user lockout.
- Passwords for accounts should adhere to Capital One's password policy.
- The application should limit file size during uploads and scan for malicious content.

Laws, Regulations, and Standards

Along with the increase of crimes, governments have started to put detailed laws and regulations to prevent and perpetrate financial criminals. Though most of the sources cover a wide variety of bank functions, many of the requirements directly affect how financial institutions should secure information and systems.

Laws

- Sarbanes-Oxley Act of 2002: This law was a response to the high amount of corporate financial fraud occurring in the early 2000's. The SOX ensures that internal controls are in place to accurately report financial activity and that those controls are monitored and logged.
- GDPR/CCPA: Recently in 2018, the General Data Privacy Regulations have been put into place and enforced by the European Parliament, European Commission and Council Member of the European Union. The law focuses mostly on data privacy which includes how companies store personal data and rights to know about breaches, use of personal data and request deletion (Trunomi, n.d.). GDPR only applies to organizations with data within the European Union. As a result, California created the California Consumer Privacy Act that echoes GDPR concepts (Eversheds Sutherland, 2019). Many state legislations are set to have their own set of regulations regarding data privacy.
- Gramm Leech Bliley Act: This law repealed the Glass-Stegall Act and was put into place to require financial organizations to provide their information-sharing practices to consumers and protect sensitive data (Federal Trade Commission, 2002).

Regulators/Regulations

- OCC: The Office of the Comptroller of Currency is a regulatory entity that audits national bank operations to ensure that they are according to laws and regulations of the government. Particularly, the OCC utilizes the Cybersecurity Assessment Tool (CAT) created by the Federal Financial Institutions Examination Council (FFIEC) to evaluate an organization's "risk and cybersecurity preparedness" (Office of the Comptroller of the Currency, 2015). Though the CAT is not a law put in place, it is incorporated in the audits that the OCC performs yearly at banks.

Standards

- PCI DSS: The Payment Card Industry Data Security Standards is a set of requirements created by the top five credit card companies to address safe ways to store, process, transmit and accept payment (Square Inc., n.d.). Though not officially enforced by a legal entity, this standard holds high precedence as those who ignore it are subject to higher fines in the event of a financial or security incident.
- OWASP ASVS: The Open Web Application Security Project (OWASP) has created the Application Security Verification Standard to help organizations secure their web applications. The standard uses verification standards to certify organizations in three levels. Requirements cover a wide variety of topics from application architecture to malicious controls (OWASP, 2016).

Control Spreadsheet

Threats / Assets(with Priority)	Disruption, Destruction, Disaster				Intrusion					Accidental	
	Fire	Flood	Power Loss	Circuit Failure	External Intruder	Internal Intruder	Eavesdropping	Web Attacks	Malware Attacks	Unintentional change	Data/system Corruption
Core Banking Database	4,5	4,5	4,5	4,5	1,2	1		1	1	4	4
Web Application (capitalone.com)					1			2,7			
Network Infrastructure					3	3	10	2			
Customer Database	4,5	4,5	4,5	4,5	1	1			1	4	4
Web Servers	4,5	4,5	4,5	4,5							
Third Party Applications								1,2			
Mail Server	4,5	4,5	4,5	4,5							
Office Spaces w/ Workstations					3	3					
Data Center Facilities	5,9	5	5, 6	5, 6	3	3					
Employees					10	11			8		
Customer Endpoints									8		

Countermeasures/Controls

1. Database Hardening
2. Input Filtering
3. Physical Security (i.e. Guards, Trap Doors)
4. Failover Servers
5. Disaster Recovery Plan
6. Separate Power System
7. Intrusion Detection & Prevention System Sensors
8. User Awareness Training
9. Fire Suppression System
10. Separate Internet Connection
11. Least Privilege Policy

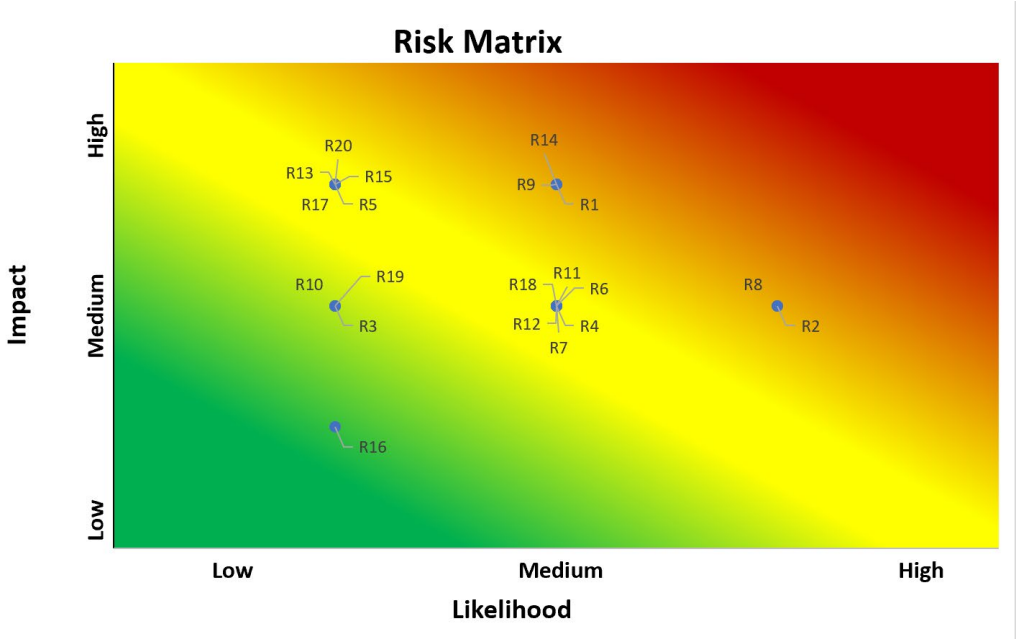
MILESTONE 2: RISK ASSESSMENT

Asset Identification

Company Assests	Type Tangible/Intangible
Company Patents (patents.justia.com/assignee/capital-one-financial)	Intangible
Capital One - Web Domain Names	Intangible
Proprietary Software (ex: Capital One mobile App)	Intangible
Capital One Trademarks	Intangible
Customer Goodwill	Intangible
Capital One Branch Buildings	Tangible
ATM Machines	Tangible
Application Data (ex: Customer Database)	Intangible
Network Infrastructure (ex: routers, cables)	Tangible
Data Center Facilities	Tangible
Employee Laptops/Desktops	Tangible
Technical Equipment (ex: mouses, headphones, keyboards)	Tangible
Employee Badges	Tangible
Mail Servers	Tangible
Web Servers	Tangible
Issued Credit Cards	Tangible
Surveillance Systems	Tangible
Office Equipment	Tangible
Third Party Agreements/Licenses (ex: AWS agreement)	Intangible
Bank Vaults	Tangible
Employees	Tangible

Risk Matrix

Risk Matrix			
Risk #	**Risk Identification**	**Likelihood**	**Impact**
R1	DDoS Attacks	2	3
R2	Malware Attacks	3	2
R3	Encryption Key compromised	1	2
R4	Broken Access Control	2	2
R5	Server Outage resulting from compromised Network Infrastructure	1	3
R6	Loss of Credit Card Information	2	2
R7	Loss of Personal Information	2	2
R8	Disclosure of Login Information	3	2
R9	Exposure of Credit Score	2	3
R10	Application Misconfiguration	1	2
R11	Corrupted Data Files from SQL Injection	2	2
R12	Masquerading during Customer Support	2	2
R13	Misuse of Employee Privileges	1	3
R14	Identity Fraud	2	3
R15	Fraudulent Activity	1	3
R16	Lapse of insurance coverage	1	1
R17	Fire in Server Room	1	3
R18	Power grid failure	2	2
R19	Leaking in Server Room	1	2
R20	Unauthorized individuals on premises	1	3



Risk Assessment

Step 1: Risk Identification	Step 2: Risk Assessment			Step 3: Risk Management					Quantitative RA				
List of Possible Risks	Likelihood H/M/L	Impact H/M/L	Consequence of the Risk (Assets Impacted)	What are we already doing about it? (mitigating factors)	What more can we do about it?	Control Classification 1 - Preventive / Detective / Corrective / Deterrent / Recovery / Compensating / Directive	Classification 2 - Technical / Administrative / Physical	Person Responsible	AV	EF %	ARO	SLE	ALE
Technical Risks													
DDoS Attacks	M	H	Servers, Web Application	Network Infrastructure with firewalls, load balancing, anti-spam	Use Virtual DNS (vDNS) to block malcious traffic (ex: CloudFlare)	Preventive, Detective	Technical	Network/Security Administrator	1000000	15	2	150000	300000
Malware Attacks	H	M	Machines/Data	Anti-malware software	Upgrade and maintain anti-malware software	Preventive, Detective, Corrective	Technical	Security Engineer	50000	10	7	5000	35000
Encryption Key compromised	L	M	Network Infrastructure, Third Party Applications	Encrypt the Encryption Key	Implement an Encryption Key Life-cycle	Preventive	Technical	Information Security Analyst	2000000	35	1	700000	700000
Broken Access Control	M	M	Application Data, Network	Role-based Authentication Control in IAM (provided by AWS)	Follow Deny by Default Control Stance in addition to RBAC	Preventive	Technical	Security Engineer	200000	20	4	40000	160000
Server Outage resulting from compromised Network Infrastructure	L	H	Mail and Web Servers	Backup hosting in addition to DNS service	Failover servers to provide operations during outages or upgrades	Corrective	Technical	Network/Security Administrator	100000	10	3	10000	30000
Loss of Credit Card Information	M	M	Customer Database, Data Center Facilities	Encrypt Credit Card details	Use Eliptical Curve Cryptography	Preventive	Technical	Information Security Analyst	300000	10	2	30000	60000
Loss of Personal Information	M	M	Customer Database, Data Center Facilities	Encryption and Tokenization of account data *Following Gramm Leach Bliley Act protocol	Using Cipher Policy- Attributed Based Encryption	Preventive, Directive	Technical	Information Security Analyst, Compliance Analyst	400000	15	2	60000	120000
Disclosure of Login Information	H	M	Third Party Applications	Multifactor Authentication - Capital One's "SwiftID" mobile app that allows confirmation/rejection of login attempts	Provide Touch ID capabilities within the SwiftID app	Preventive	Technical	Security Engineer	50000	60	3	30000	90000
Exposure of Credit Score	M	L	Customer Database, Data Center Facilities	Capital One's "CreditWise" data is encrypted with 256-bit Transport Layer Security (TLS).	Upgrade TLS protocol to TLS 1.3 and continue to update "CreditWise" Application	Preventive	Technical	Security Engineer	400000	15	2	60000	120000
Application Misconfiguration	L	M	Third Party Applications	Use-case testing and code reviews	Implement a patch management tool to promote accountability and store info such as the "who, when, where" of code changes	Preventive, Detective	Technical, Administrative	Software Testers and Programmers	80000	50	1	40000	40000
Corrupted Data Files from SQL Injection	M	M	Core Banking Database, Customer Database	Storage of backup data files on physical and "cloud" servers	Limit use of Dynamic SQL and continously monitor database connections	Corrective, Recovery	Technical	Security Engineer, Database Administrators	1000000	22	2	220000	440000
Business Risks													
Masquerading during Customer Support	M	M	Customer Database, Customer Endpoints	Capital One Support agents will follow procedures to verify Customer identity and will not ask for banking password or answers to online security questions.	Live video-chat solutions to add an extra layer of verification	Preventive, Directive	Administrative	Customer Support Agents	65000	15	5	9750	48750
Misuse of Employee Priviliges	L	H	Employees, Network Infrastructure, Core Banking Database	Employees follow Acceptable Use Policies	Separation of Duties	Preventive, Directive	Administrative	Security Managers	30000	5	4	1500	6000
Identity Fraud	M	H	Customer Database, Core Banking Database, Customer Endpoints	"Confyrm" from Capital One provides identity verification services through use of IDs, mobile network information, consumer information databases, device confidence and risk evaluation	Dark web scanning for stolen credentials and bank account information such as credit card numbers, etc.	Preventive	Technical	Security Engineer	50000	10	10	5000	50000
Fraudulent Activity	L	H	Core Banking Database	Capital One Customer Support responds by freezing accounts and alerting vendors	Training agents on trending fraud activities happening around the world	Corrective	Administrative	Customer Support Agents	25000	5	4	1250	5000
Lapse of insurance coverage	L	L	Customer Goodwill	Ensuring consistant coverage by not changing coverage and keeping up with payments	Allocating monetary resources needed to keep up with payments	Compensating	Administrative	Accountants and Finance department	10000000	10	1	1000000	1000000
Physical Risks								x					
Fire in Server Room	L	H	Data Center Facilities, Servers	Halon Substitute Fire Supression System since sever room full of electrical equipment	Supression system should be maintained and routinely tested.	Corrective	Physical	Building/Server Room Manager	5000000	35	1	1750000	1750000
Power grid failure	M	M	Data Center Facilities, Servers	Backup generators	Charge the generator cyclically to perserve functionality	Corrective	Physical	Building/Server Room Manager	3000000	50	2	1500000	3000000
Leaking in Server Room	L	M	Data Center Facilities, Servers	Water detection sensors	Raise the floor the servers are on and have water drain	Detective	Physical	Building/Server Room Manager	180000	20	1	36000	36000
Unathorized individuals on premises	L	H	Data Center Facilities, Servers	Security cameras (CCTV) and guards monitor Capital One buildings and server rooms	Biometric scanners (ex: finger print reader) to access certain rooms	Preventive, Detective, Detterent	Physical, Administrative	Security Guards	15000	10	3	1500	4500

Key Security Roles

- Senior Management
    - Chief Information Security Officer (CISO): Michael Johnson
        - Vice President, Information Security and Deputy CISO: Aaron Hughes
- Data Owners
    - Executives
    - The Company
- Custodians
    - Database Administrators
    - Engineers
        - Cybersecurity
        - Network
    - Cybersecurity Analysts
    - Helpdesk and Computer Technicians
    - 3rd Party
        - Consultants/Contractors
        - Pen Testers/Ethical hackers
        - Datacenter Cybersecurity Team
        - Datacenter Security Guards

Key Stakeholders

- Internal Stakeholders
    - Employees
    - Shareholders
        - Majority
        - Minority
- External Stakeholders
    - Customers
        - Corporate
        - Retail
    - Government
        - Federal
        - State
        - Local

MILESTONE 3: SECURITY POLICY

Introduction

As a leader in the personal finance industry, Capital One takes extreme pride in keeping personal information safe, and out of the hands of unauthorized users. The policies covered in this security policy have been created to prevent and mitigate any theft of personal information due to unauthorized access to the company's assets. The purpose of these policies is to give employees, contractors, and vendors, a reference on how to conduct day to day operations in a safe and secure manner. Topic covered in this policy range from internet policy down to anti-virus policy. Breach of any aspect of this policy will be subject to discipline and any persons responsible will be reprimanded based on each guideline.

Outlined in this document is policies that will help prevent and mitigate unauthorized people from accessing confidential and restricted information. Included are the list of policies regarding the Internet, system usage, and anti-virus, [physical security, acceptable use, email and password]. Security requirements, goals, and scopes as well as the risks and the priorities of those risks. This policy also defines what is confidential, public, restricted, and internal information is and what could happen if any of that information is accessed.

Security Requirements, Goals and Scope

2.1 Requirements

Capital One assets (physical, personnel, data, IT operations) must be protected from range of common and advanced cyber threats. Key areas of concern that need to be addressed are internet usage, system usage, malicious computer software, unauthorized access to company devices and locations, sensitive information leak via forms of communication such as emails and internal collaboration platforms (i.e. Skype, Teams), unauthorized usage of company data, and lastly exploitable credentials. The company must have redundant security countermeasures and failovers/ backups in case of a cyber-attack. Internet usage must be restricted to where various websites are denied access for numerous reasons such as websites hosting malware, inappropriate content, content that lead away from employee productivity and more. The network must be segmented so that general internet access doesn't grant access to intranet content from outbound to inbound traffic and thus prevent unauthorized parties to access data behind company IPs and websites. All Capital One devices, servers, workstations, phones, tablets, laptops, and more must be safeguarded against malicious software via an anti-virus application. Physical and electronical safeguards such as fences, security guard post, badge-in doors, circulating doors, and more must be enabled at all company property to prevent unauthorized access and impersonation or social engineer attacks. Employees must be trained on and made aware of acceptable actions using company devices and network, and must understand consequences of failing to abide by them. Safeguards must be in place to prevent unauthorized access to sensitive data as well as enable IT safeguards preventing data exfiltration of critical data via various forms such as email, and other inner company communication methods. Lastly, every device must be password protected and require strong credential for authorized access.

2.2 Goals

Security requirements are to be used to create specific tasks and processes that help better protect Capital One as a whole. The requirements outlined in 2.1 must be adhered to the best of ability

by all personnel. Doing so is important as these are designed to protect Capital One and all of its assets (physical, personnel, data, IT operational, and more) against numerous threats such as unauthorized data access to PII of employees and customers, social engineering and impersonation attacks, severe disruptions to company operations, and any threats to the confidentiality, integrity, and availability of company data and operations. All employees are to be trained with respect to the above-mentioned requirements so they can help facilitate the procedures and further help the company stay secure.

2.3 Scope

The scope of this document and its defined requirements, goals, and policies are to set a clear standard of acceptable and unacceptable actions and scenarios. It serves as a guide to help the staff be aware of when they are infringing company policies and possibly exposing it to security vulnerabilities that may be exploited as well as stay vigilant of others doing that. Below policies in section 5 further break down acceptable system and internet usage, methods to protect company devices from malicious programs, appropriate company communication via email and other communication platforms, control over access to data, and lastly effective credentials to safeguard all company devices and domains.

Information Classification Map for Capital One

Figure 1 is a model representing the classification of data and information at Capital One. The 4 levels are ranked based on impact and security requirements. The first 3 layers (Restricted, Confidential, Internal) of information are based on sensitive information.

The impact level increases from the Public layer to the Restricted layer. Impact reflects the consequences faced when there's breach or disclosure of sensitive information.

Additionally, the protection that is required increases from the Public layer to the Restricted layer.

Employees should have the proper clearance to access labeled information.

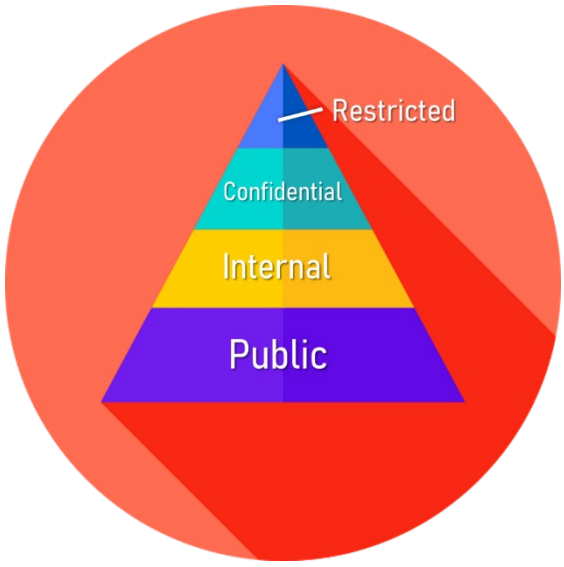


Figure 1

Table 1 discusses the types of information under each information layer. It also provides an outlook on some of the impacts Capital One faces if the categorized information was breached.

Restricted	Types of Information: • Encryption keys • Server passwords • Back up data Impact: • Compromised databases, networks, devices • Collapse of major operations

Confidential	Types of Information: • Customer data - credit card numbers, transaction history, credit scores, and account balances • Personal Identifying Information (PII) of customers and employees – Social Security Numbers Impact: • Heavy damages/fines (ex: Violation of Gramm Leach Bliley Act) • Compromised accounts • Class action lawsuits
Internal	Types of Information: • Customer and market research data • Proprietary software (ex: Capital One app code) • Vendor agreements • Network passwords (ex: WiFi password for Tulsa branch) • Human resources data Impact: • Loss in competitive advantage • Minimal litigation involved • Decreased employee trust
Public	Types of Information: • Financial Statements (Quarterly, Annually) • Accounting Audits • Issues and outstanding stock transactions • Company statistics (ex: Number of employees, number of ATMS, location of banks/headquarters) Impact: • No financial harm involved • Influences decisions made by investors • Helps public perception of the company

Table 1

Restricted Information

It is our number one priority to provide safeguards and protective measures for the information in this category. Employees with access to this type of information are vetted carefully and nonrepudiation is followed. Our encryption keys, server passwords, and back up data are encrypted to prevent breaches. Data in motion as well as data at rest is encrypted using advanced technologies.

Confidential Information

Customer information and PPI are protected to a high degree. We want to respect our customer's decision to entrust us with their information, therefore we use industry leading technologies to protect it. One example of our practices is using digital signatures, which identifies who's making the request to access customer information. Additionally, when our customers connect to a support representative, the session between the two is encrypted using 128-bit Secure Socket Layer (SSL). Our employees are knowledgeable and actively ensure security policies are being followed. We respect and comply with the legislation of the countries we conduct business in.

Internal Information

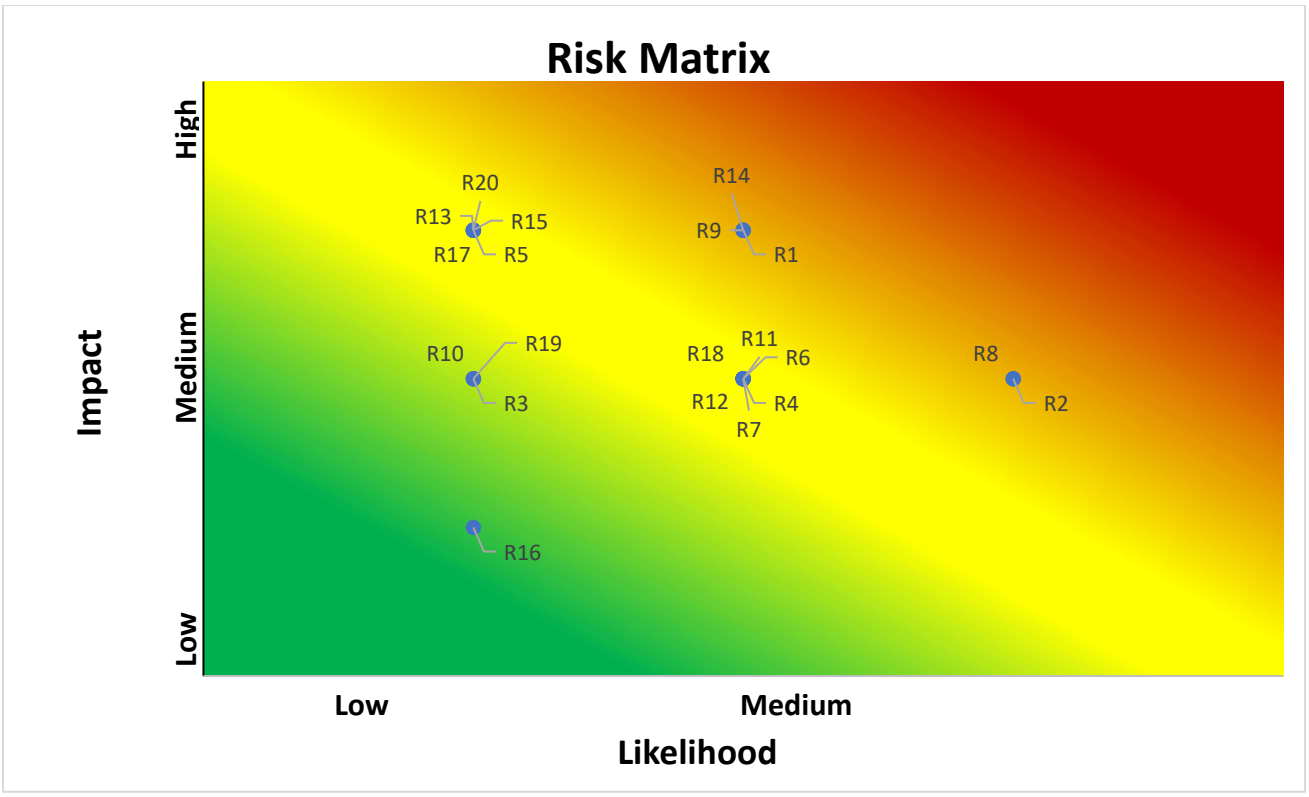
The day to day duties conducted by our employees and contractors often involve exposure to internal information. It is our priority to allow only authorized access to such information. To ensure proper authorization, we use an Identity Access Management (IAM) service. Its capabilities include multifactor authentication and reporting of suspicious login activity. Additionally, role-based access control (RBAC) is observed and the roles parallel those within the organization. Our RBAC configurations allow confidentiality of the information we store and collect at Capital One. Capital One's Critical Stack, which is a platform for orchestrating development and deployment of enterprise software, offers RBAC solutions for internal company needs.

Public Information

We understand that as a publicly traded company, there are certain financial statements and documents we must publish to the public. To provide potential investors and customers with legitimate and reliable information we often undergo audits by the world's top auditing firms. Capital One takes measures to verify the released information is "Public" and not under the other 3 layers before it is released to public. Oversight of disclosed information is valuable to us especially due to competitive risks imposed by other banks. Transparency is important as well, and we believe our customers should have the right to be aware of any key events whether it is security incidents or lawsuits.

Risks and Risk Matrix

Risk Matrix			
Risk #	**Risk Identification**	**Likelihood**	**Impact**
R1	DDoS Attacks	2	3
R2	Malware Attacks	3	2
R3	Encryption Key compromised	1	2
R4	Broken Access Control	2	2
R5	Server Outage resulting from compromised Network Infrastructure	1	3
R6	Loss of Credit Card Information	2	2
R7	Loss of Personal Information	2	2
R8	Disclosure of Login Information	3	2
R9	Exposure of Credit Score	2	3
R10	Application Misconfiguration	1	2
R11	Corrupted Data Files from SQL Injection	2	2
R12	Masquerading during Customer Support	2	2
R13	Misuse of Employee Privileges	1	3
R14	Identity Fraud	2	3
R15	Fraudulent Activity	1	3
R16	Lapse of insurance coverage	1	1
R17	1.1.1 Fire in Server Room	1	3
R18	Power grid failure	2	2
R19	Leaking in Server Room	1	2
R20	Unauthorized individuals on premises	1	3


Risk Matrix
Impact
High
Medium
Low
R20
R13
R15
R17
R5
R14
R9
R1
R10
R19
R3
R18
R11
R6
R12
R4
R7
R8
R2
R16
Low
Medium
Likelihood

Policies

Internet:

1.1.2 Employees, vendors, and contractors are only allowed to access websites related to work and that are not restricted by any filters while using any internet service provided by Capital One.

1.1.3 Any person that violates this policy will be reprimanded by verbal warning up to and including termination.

1.1.4 No one is allowed to access any Capital One assets using any connection other than one provided by Capital One.

1.1.4.1 Failure to follow this policy can result in immediate termination

1.1.5 Typing user credentials in on unauthorized websites is prohibited. Always verify any websites that look similar to company websites, but look slightly different, with IT to ensure the correct website is being accessed.

1.1.6 Failure to comply with this policy will result in password changes for all user accounts associated with Capital One.

1.1.7 No employee, vendor, or contractor will use Capital One internet to download, stream, or upload any games, movies, music, or personal files that are not related to work or Capital One during or off work hours.

1.1.8 Any person that is found to be uploading, downloading, or streaming unauthorized files will be reprimanded.

1.1.9 No object that can connect to a wired or wireless connection is allowed to connect to the internet service that Capital One uses, unless authorized by IT.

1.1.10 Any unauthorized connections will be terminated and the person responsible will be disciplined by verbal warning and face possible termination.

1.1.11 Please report any object that appears that looks like it doesn't belong to capital one or looks suspicious, to the IT and the Information Security team for further investigation

1.1.12 No customer is allowed to access any portal but the customer web application and the mobile app.

1.1.13 Failure to comply with this policy can result in an account lock and possible ban from using any online functions for the account.

1.1.14 Capital One holds the right to monitor internet traffic and terminate any unauthorized connections without prior notice

System Usage:

1.1.15 System usage policy applies working at Capital One sites, remotely or using personal internet connection to access Capital One systems. Limited personal use of Capital One systems is allowed, although it must not negatively impact the user's performance in completing its task, break any of Capital One's policies, use a lot of resources, and/or increase cyber insecurity.

Usage Surveillance

1.1.16 Capital One has the right to surveil, assess, audit, interrupt, access, and reveal any data stored, formed, received or sent using Capital One System.

Hardware and software

1.1.17 Only Capital One issued computer hardware and devices are allowed to be connected to Capital One Corporate network. Personal devices can be connected to Guest Network after users have taken a reasonable step towards ensuring that the device is malware, and virus protected. Flash Drive can be used but must be encrypted in it contains sensitive information.

1.1.18 Software that is approved and licensed by Capital One is to be installed on Capital One systems. Likewise, only authorized cloud services can be used on Capital One business purposes. Users who download files, software, or use unauthorized cloud service maybe financially liable for the damage that cloud incur from viruses and unlicensed software.

Remote Access

1.1.19 All sensible caution must be exercised to guarantee that any device being utilized to connect to Capital One Systems is free from spyware and viruses by securing the device has installed a suitable firewall and antivirus security. Users of Capital One Systems must guarantee that devices are not left abandoned or put in a place or situation where unauthorized access could transpire.

Security

1.1.20 Unique usernames and passwords are utilized to access Capital One's Systems, and multi-factor authentication (MFA) tokens are also required. Passwords are required to be changed regularly when prompted at login, as explained in our password security policy. Access to sensitive systems such as ERP and Payroll will be evaluated regularly.

Anti-Virus

1.1.21 All Capital One PC-based computers must have Capital One’s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the antivirus software and the virus pattern files must be kept up-to-date. Any activities with the intention to create and/or distribute malicious programs into Capital One’s networks are prohibited, in accordance with the Acceptable Use Policy.

1.1.22 The Security Operations Center is responsible for creating procedures that ensure antivirus software is run at regular intervals and computers are verified as virus-free.

Physical Security

1.1.23 All Capital One premises must be restricted to authorized employees only. Adequate safeguards (defined in 5.4.2) must be in place to enforce the physical security requirements all throughout the company.

1.1.24 In order to control company premises access, military grade lock system must be implemented and functional at every door. Depending upon the severity of contents of data and operation in a certain room, the entry must be protected from simple badge scan access to a combination of badge-in (something you have), iris scan (something you are), and a passcode entry (something you know). A confirmed identity is crucial to gaining access to company property.

1.1.25 Entrance for all building will include a badge-in along with a 24/7 security guard. After hour access will be limited only one entry point where the guard is stationed.

1.1.26 High resolution CCTV cameras of various type, wide angle, dome camera, infrared, motion-detecting, are required to be installed at all entry and exit point, hallways, and general rooms depending upon the location. These will feed into the security officer's post at all times over an enclosed isolated network preventing any tampering of the feed.

1.1.27 Adequate lights are to be installed in parking lots, outside of buildings, dark corners and camera blind spots, and lastly throughout the inside of the building so the security staff can easily identify unauthorized personnel on the property.

1.1.28 Special buildings such as data centers and security operations center are to have dual trap door system or the circulating lock doors to capture the individual attempting an unauthorized entry.

1.1.29 All workstations are to be locked or bolted down to the respective office or cubicle in order to prevent attempts to steal company devices and the data stored within them.

1.1.30 Server racks or other critical devices are to be isolated from the room access using a locked device cage that can be opened only using a certain key.

1.1.31 Sprinkler systems are to be installed as per city fire regulation in order to prevent a fire from spreading. Additionally, clearly visible signs with direction to a fire extinguisher are required.

1.1.32 In settings where critical systems are operating or where devices pose a risk of electrical failure, fire suppression system is to be non-liquid based so that the unimpacted machines can continue operating.

Email Policy

1.1.33 Use of email must follow with Capital One's policies and procedures and comply with applicable laws and proper business practices

1.1.34 Capital One email accounts should be used primarily for Capital One business related purposes; personal communication is permitted on a limited basis, but non-Capital One related commercial uses are prohibited

1.1.35 All Capital One data contained within an email message or an attachment must be secured according to the Capital One's Data Protection Standard.

1.1.36 Email should be retained only if it qualifies as a Capital One business record. Email is a Capital One business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

1.1.37 Email identified as a Capital One business record shall be retained according to Capital One's Record Retention Standard.

1.1.38 The email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs or national origin. Employees who receive any emails with this content from any Capital One employee should report the matter to their supervisor immediately.

1.1.39 Users are prohibited from automatically forwarding Capital One emails or business records to third party email systems. Individual messages which are forwarded by the user must not contain Capital One confidential or above information.

1.1.40 Users are prohibited from using third party email systems and storage servers such as Google, Yahoo, Dropbox, etc. to conduct Capital One business, to create or memorialize any binding transactions, or to store or retain email on behalf of Capital One. Such communications and transactions should be conducted through proper channels using Capital One approved documentation.

1.1.41 Using a reasonable amount of Capital One resources for personal emails is acceptable, but non related work email shall be saved in a separate folder from work related email.

1.1.42 Sending chain letters or joke emails from a Capital One email account is prohibited.

1.1.43 Capital One employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Emails are subject to review in the case of an audit finding or investigations Capital One initiates.

1.1.44 Capital One may monitor messages without prior notice. Capital One is not obliged to monitor email messages.

Data Usage

1.1.45 Any data stored on Capital One issued laptops or sent across Capital One networks may be collected and retained for internal or external investigations.

1.1.46 Any employee identifiable data will not be used to make a profit and will only be disclosed in accordance to the appropriate laws.

Password Policy

Password Creation

1.1.47 Passwords must adhere to the Capital One's internal Password Construction Guidelines

1.1.48 Work passwords should be unique and used only for work-related accounts. Users may not use a password that is utilized in non-work-related accounts.

1.1.49 For user accounts that have a higher-level of access, a separate and unique password must be used to access the account.

Password Change

1.1.50 A password change should only be initiated in the event that it is compromised or is not in adherence to the standard.

1.1.51 Random scans may be performed on user account passwords by the Identity Access Management department to ensure unique password usage between a regular and high-level access account or prevent use of common passwords.

Password Protection

1.1.52 Passwords to work-related user accounts must never be shared with anyone and must be treated as sensitive data.

1.1.53 Passwords must not be communicated via text or email or in any form of digital communications.

1.1.54 Passwords must not be written down and stored near user's cubicle or desk.

1.1.55 Passwords may be saved utilizing a Vendor Onboarding approved password storage application.

1.1.56 When using Google Chrome, Mozilla Firefox or any other browser, a user must not opt to choose "remember password".
1.1.57 In the event that a password is compromised, the user should report the details to cybersecurity@capitalone.com and change all passwords to current accounts.

Multi-factor Authentication

1.1.58 Multi-factor Authentication must be used in conjunction with passwords to log into high-level access accounts.
1.1.59 Multi-factor Authentication is optional for user-level access to applications or services but is highly suggested to take advantage of.

Acceptable Use

1.1.60 The information that is collected and stored within Capital One systems and devices is the property of Capital One. The information may belong to customers, vendors, and employees.
1.1.61 Date stored on Capital One's devices should be protected and managed in compliance with legislation and standards viable to Capital One.
1.1.62 You need to value integrity and take proper action when you have suspicion of or have identified an event in which the security triad (Confidentiality, Integrity, Availability) is violated.
1.1.63 You must follow Capital One's security training and practice due diligence when carrying out responsibilities involving proprietary information.
1.1.64 Capital One's employees should understand the extent of the legislation and standards viable to Capital One.
1.1.65 You may utilize collected and stored information as long as there is proper authorization and it correlates with your roles and receptibilities.
1.1.66 You must be aware of who to contact when there is a violation of the security triad and follow given protocols.
1.1.67 The Capital One device you use on premises or offsite may be monitored for security purposes at any given time. These devices should not be used to collect or store any information unrelated to business operations.
1.1.68 Only Capital One devices may be used to conduct your roles and responsibilities. These devices should not be placed or used in unauthorized locations.
1.1.69 When collecting information, ensure that it is coming from an authorized source whether it is a customer or a fellow employee.
1.1.70 Raise awareness of Capital One's security standards when collecting information from current and potential customers.

Policy Compliance

1.1.71 The Information Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.
1.1.72 Any exceptions to the policy must be approved by the Information Security team in advance.
1.1.73 An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Responsibilities

Responsibilities	
Policy	**Enforcer**
Internet	System Administrator Department
System Usage	System Administrator Department
Anti-Virus	Information Security Department
Physical Security	Information Security Department
Acceptable Use	System Administrator Department
Email Policy	System Administrator Department
Data Usage	System Administrator Department
Password Policy	Information Security Department

Team Meeting Minutes

Meeting Number	Meeting Date	Time Start	Time End	Members Present	Objectives Discussed	Other Notes
1	Monday, September 2, 2019	12:00 pm	2:05 pm	Sarah, Arsalan, Vraj, Reece, Steve (All)	• Milestone 1 requirements • Potential Companies • Selection of Capital One • Previous Security incidents • Potential threats & risks • Laws, policies involving Capital One • Capital One business model • Capital One's security roles and stakeholders • Risk Assessment Template	-Assigned Milestone 1 responsibilities
2	Thursday, October 10, 2019	5:10 pm	6:10 pm	Sarah, Arsalan, Vraj, Reece, Steve (All)	• Milestone 2 requirements • Identifying new Assets • Review of Risk Types • SLE/ALE Formulas • Risk Matrix structure • Laws applicable to Capital One • Current Countermeasures/controls	-Assigned Milestone 2 responsibilities
3	Saturday, November 2, 2019	11:00 am	11:40 am	Sarah, Arsalan, Vraj, Reece, Steve (All)	• Milestone 3 requirements • Looking at possible policies • Existing Information security policies for Capital One • Examine other companies' policies	-Assigned Milestone 3 responsibilities

Recorded by Steve John

Works Cited

Capital One. (2019a). Explore Credit Cards & Apply Online. Retrieved from https://www.capitalone.com/bank/money-management/banking/online-banking-services/

Capital One. (2019b). The Benefits of Online Banking Services. Retrieved from https://www.capitalone.com/bank/money-management/banking/online-banking-services/

Capital One Financial Corp. (2019). 2018 Annual Report. Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=70667&p=irol-irhome

Eversheds Sutherland. (2019). California Consumer Privacy Act. Retrieved from https://www.californiaconsumerprivacy.com/

Federal Reserve System. (2019, March 31). Large Commercial Banks. Retrieved from https://www.federalreserve.gov/releases/lbr/current/

Federal Trade Commission. (2002). How to comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach Bliley Act. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

Krebs, B. (2019, July 30). Capital One Data Theft Impacts 106M People. Retrieved from https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/

Office of the Comptroller of the Currency. (2015). Cybersecurity: FFIEC Cybersecurity Assessment Tool. Retrieved from https://occ.gov/news-issuances/bulletins/2015/bulletin-2015-31.html

Office for Victims of Crime. (2018). 2018 NCVRW Resource Guide: Crime and Victimization Fact Sheets. Retrieved from https://ovc.ncjrs.gov/ncvrw2018/info_flyers/fact_sheets/2018NCVRW_FinancialCrime_508_QC.pdf

OWASP. (2016). Application Security Verification Standard 3.0.1 [PDF]. Retrieved from https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

Reuters. (2019). Capital One Financial Corp (COF.N) Company Profile. Retrieved from https://www.reuters.com/finance/stocks/company-profile/COF.N

Square, Inc. (n.d.). PCI Compliance: What You Need to Know. Retrieved from https://squareup.com/guides/pci-compliance

Trunomi. (n.d.). EUGDPR. Retrieved from https://eugdpr.org/the-regulation/