Individual Assignment - Security Assessment Report (SAR)

137:561 Essentials of Cybersecurity and Secure Systems

Isaac S Yoon

April 22nd, 2023

Professor Steven H Richman

Rutgers University

SECURITY ASSESSMENT REPORT (SAR)

JPMorgan Chase & Co

Financial Services & Banking Industry

April 22, 2023

SECURITY ASSESSMENT

1. Background:

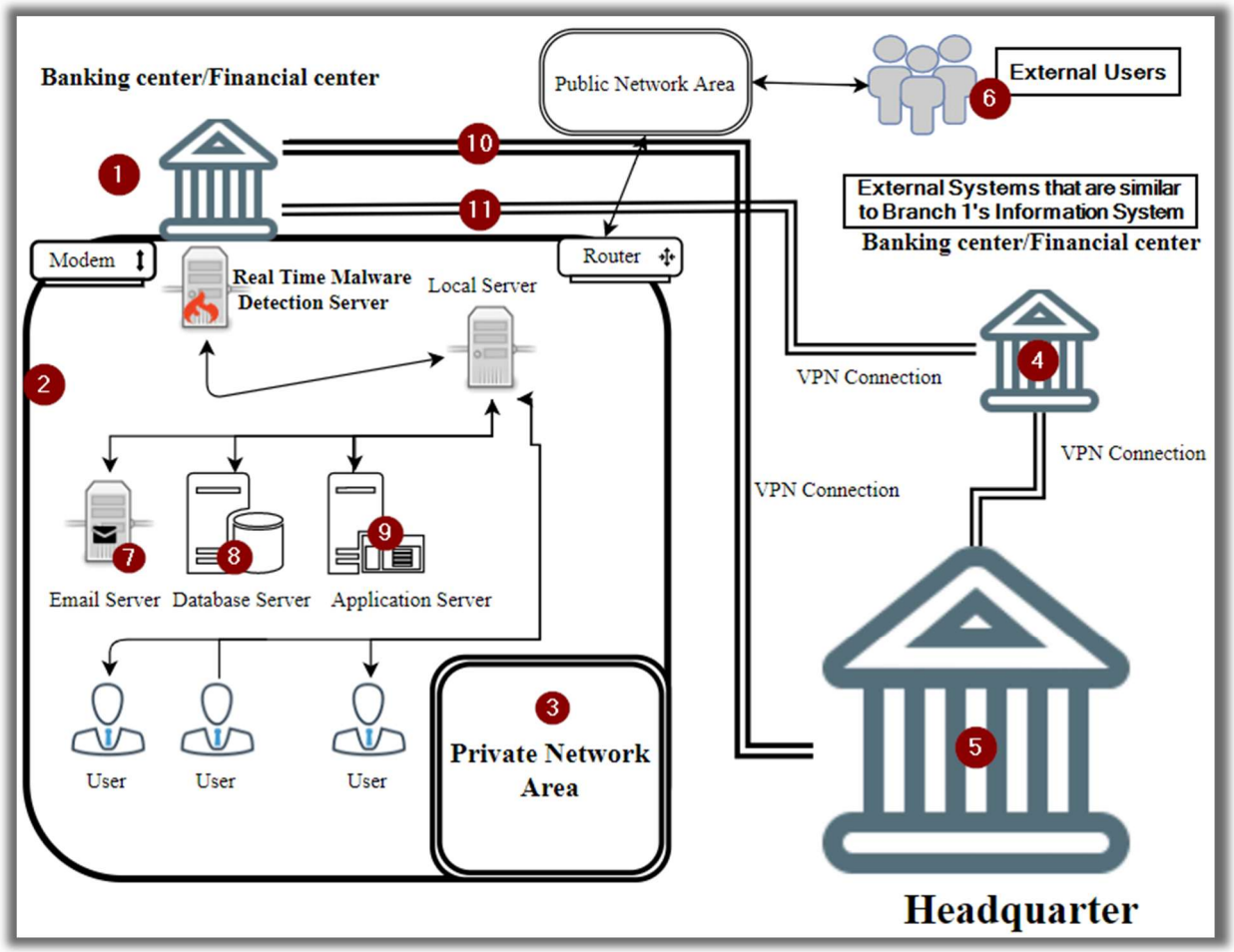
1.1 Purpose:

After recent news of the U.S. Office of Personnel Management's data breach, it is of utmost importance that J.P. Morgan Chase & Co. conducts an annual audit of our organization's cybersecurity program. This Security Assessment Report aims to assess our company's current cybersecurity program for strengths and weaknesses in the current fiscal year. In addition, auditing the company's cybersecurity program will determine if it is in compliance with the Federal Information Security Modernization Act of 2014. This Security Assessment Report examines our Critical Information Systems, the threats and vulnerabilities to our Critical Information Systems, and different means for remediation from our team. Our goal after this assessment is to determine if our company represents an "effective" level of security according to the maturity model, Level 4(Managed and Measurable), prepared by the Office of Management and Budget and the Department of Homeland Security (Department of Health and Human Services (HHS), 2021, pp. 1-3).

1.2 Organization:

J.P. Morgan Chase & Co. is one of the world's oldest and largest publicly traded companies. Within the Financial Sector, J.P. Morgan Chase & Co. is separated into three divisions: banking, financial services, and investment banking. J.P. Morgan Chase & Co serves clients globally with various services within our three divisions. These financial services include but are not limited to investment banking, personal/business/commercial banking, treasury and securities services, asset management, and corporate financial services (J.P. Morgan Chase Profile | Street of Walls, n.d.). J.P. Morgan & Chase has over 200 years of experience and over $2.6 trillion in assets (Our Business, n.d.). With our industry's highly valued assets and data (PII, PI, SPI, etc.), we align with industry standard cyber security practices including Network Security and Surveillance, Software Security, Risk Management, and Protecting Critical Information Systems (Naz, 2023) to mitigate security threats targeting our banks, financial services, and highly sensitive information.

1.3 Critical Information Systems:



This graph contains an overview of one of our company's offices[1]. Within the graph, you are able to see an expanded view of how external users[6] and systems[4,5] are connected to the first office. Our Private Network Area[3] connects to the router and modem, which can then be used to be connected to the Public Network Area (the first communication network residing outside of our company's firewall[2]). The most important aspect of our Information System is that inside our Private Network Area, you can see the users that are requesting data from the Local Server. The Local Server passes the request to the Real Time Malware Detection Server to capture any malicious activity. Then the RTMDS approves of the request, then the Local Server submits multiple queries to the Email Server, Database Server, or Application Server, where the data rests[7,8,9]. These result sets are then provided to the user. Since our company uses a distributed computing system, our system must communicate through the VPN connection to the other branches and our Headquarters[10,11]. This allows for our information systems to contain the same data of an account balance after a withdrawal/deposit and more.

2. Assessment Approach:

2.1 Very brief review of OPM Breach(s):

In the 2020 Fiscal Year, the Office of Inspector General contracted Ernst & Young LLP to conduct a performance audit of the Department of Health and Human Services' compliance with the Federal Information Security Modernization Act (FISMA) of 2014. As of September 30th, 2020, OIG concluded that the evaluation of HHS did not meet the required maturity level for the Cybersecurity Framework five function areas, which were defined by the FISMA metrics, and deemed "Not Effective" (OIG, 2021, pg. 1, 3, 5).

In the Department of Health and Human Services Federal Information Security Modernization Act Report, section three consolidated all the findings identified at each of the selected Operation Divisions reviewed against the Cybersecurity Framework's five function areas. For example, one of the findings reported that one selected Operation Division failed to complete a security impact analysis (SIA) while implementing the change of HHS information systems (***Identify Function, Risk Management Domain***). As a result, the changes made to each system did not acknowledge any security threats or impacts. Additionally, an OpDiv was unable to provide evidence of documentation that two specific systems, owned/operated by a contractor, requested, or approved any changes made to those two systems (***Protect Function, Configuration Management).*** There was also no evidence of contractors complying with established screening criteria and contractual agreements, nor did OpDiv conduct periodic review for the adjustments of privileged user account and permissions (***IAM Domain***). Lastly, another main concern discussed in the report was the finding identified in the HHS' incident response program. This finding included that improvements could be made to the criteria that assess and determine the incident level based on its impact (pg. 9-20).

2.2 Relevance of OPM Breach(s) to J.P. Morgan Chase & Co:

The impact of the 2015 OPM Data Breach resulted in 21.5 million current, former, and prospective Federal employees and contractors having their background investigation records stolen. The background investigation records contained highly sensitive information such as full names, birth dates, home addresses, and Social Security Numbers (OPM, n.d.). The OPM Data Breach is relevant to any organization because it highlights the consequences of a large-scale cyber-attack. However, this breach is specific to J.P. Morgan Chase & Co. because of the organization's access to personally identifiable information (PII) entrusted to us by our clients. J.P. Morgan Chase & Co and all its subsidiaries are subjected to Federal Regulations that they *must abide by* to ensure data privacy, confidentiality, and data protection. After reviewing this report, J.P. Morgan Chase & Co. must assess our security systems and implement preventative measures for future cyber-attacks. As a result, will reduce the risk of future data breaches and minimize the potential threats and vulnerabilities to the assets of J.P. Morgan Chase & Co.

3. Assessment Results[1]:

3.1 Insider Threats:

ID	Threat	Synopsis	Impact[2]
IT1	Negligent Employees/Contractors: (Specifically: Use of unauthorized software/devices) (Gibbons, n.d.)	Negligence is not always malicious. Negligent practices include employees/contractors using unauthorized software. This includes third party software that employees don't want to pay for, and the software can be pirated.	This can lead to unauthorized access. An example would be using unauthorized software that leads to malware.
IT2	Lack of Access Control: Unauthorized Access (Richman, 2023)	Inside actors(malicious) may use system flaws to access systems that they are not authorized for.	This can lead to attackers gaining sensitive information such as login credentials or data.
IT3	Use of Old/Outdated Hardware (Richman, 2023)	Companies may not be budgeting properly for newer equipment. With older equipment, you can be using older Operating Systems and older software. These products can be considered an EOL (end of life product) product.	This can lead to the susceptibility of malware. Since older software can no longer be supported, it can have more vulnerabilities with no maintenance or updates.

3.2 External Threats:

ID	Threat	Synopsis	Impact[2]
ET1	DDoS Attacks (Martin, 2023)	Distributed Denial of Service Attacks is when attackers direct traffic to overwhelm a system with requests to the database that it becomes unavailable.	This can lead to larger impacts and is typically used as a distraction for larger scaled attacks.
ET2	Brute Force Attacks	As seen in Cain and Abel, BF Attacks attempts every possible combination of characters until the right password is found.	Brute Force attacks can allow unauthorized access to information systems, data, and more.

[1] For critical system(s), data/information, networks, and interfaces to external systems and users.
[2] Quantify or provide recent relevant examples or incidents of business, safety, health… impact.

	(Richman, 2023)		
ET3	**SQL Injection (BasuMallick, 2022)**	**Structured Query Language injection is the technique where attackers can identify a vulnerable SQL-driven website, then inject malicious SQL queries. This query is then validated, and the command is executed by the database.**	**This attack can be utilized to manipulate back-end databases to query for confidential data.**

3.3 Vulnerabilities[3]:

ID	Vulnerability	Synopsis	Impact[2]
V1	**Lack of Data Encryption Measures (Namuag, 2021)**	**Database encryption converts data in the database to cipher text using different algorithms. There are two important types of encryptions: Data at-Rest Encryption/Data in-Transit Encryption.**	**Without database encryption, unauthorized users will be able to access data across the entire system. Can impact the susceptibility to attacks such as SQL Injection, Man in the Middle attacks, or cross-site scripting.**
V2	**Lack of Malware Detection Software/Systems**	**Malware Detection Software/Systems is a good *reactive* approach to system vulnerabilities. Strong security measures can still be compromised and lead to vulnerabilities.**	**Without Malware Detection Software/Systems, the organization will not be able to detect malware. The impact can lead to data loss and data integrity.**
V3	**Lack of Database Backup**	**Database backup is the copy of an organization's structured data.**	**The impact of not having a database backup is the loss, corruption, or damaging of files in the database. These files will be hard to recover.**

[3] Include results from all lab testing (e.g., MBSA OS and password cracking assessments, as well as your paper analyses.

4. Assessment Results:

4.1 Cybersecurity Assessment of Threats and Vulnerabilities:

ID[4]	Threat or Vulnerability[1]	Current Security Posture	Deficiencies in Current Posture
IT1	Negligent Employees/Contractors: (Specifically: Use of unauthorized software/devices) (Gibbons, n.d.)	There is a strong security posture currently determined by our implementation of Group Policy. Group Policy is considered a security measure that will provide specific configurations for users/PCs.	Although our organization implements a Group Policy that aligns with the industry standard policies, there is a lack of auditing for our Group Policy changes.
V1	Lack of Data Encryption Measures	Our organization has an efficient Virtual Private Network that users/other systems are connected to. Our VPN is an encrypted connection that safely transmits sensitive information/data.	As shown in the Network Diagram in Section 1.3, there is no evidence of encryption for Data at-Rest.
V2	Lack of Malware Detection Software/Systems	Shown in the Network Diagram, there is a Real-Time Malware Detection dedicated server that scans the Local Server live.	There is currently only one Real-Time Malware Detection Server that can be susceptible to external threats.
V3	Lack of Database Backup	Our network has a low security posture regarding backup databases. As shown in the Network Diagram in Section 1.3, there are no present backups.	Our network does not present a backup of any of the three databases in the diagram. This is a major security concern as these database files can be corrupted, damaged, or changed in the event of an attack.

[4] Use the corresponding IDs (e.g., IT2, ET1, V3) you provided in the tables, above.

5. Potential Security Measures:

ID[4]	Current Security Posture [from Table 4.1]	Deficiencies in Current Posture [from Table 4.1]	Potential Security Mitigation Techniques
IT1	There is a strong security posture currently determined by our implementation of Group Policy. Group Policy is considered a security measure that will provide specific configurations for users/PCs.	Although our organization implements a Group Policy that aligns with the industry standard policies, there is a lack of auditing for our Group Policy changes.	Aside from enabling the audit of Group Policy changes using Security Event Logs, administrators need to provide evidence of configuration changes made to a local machine. Also, two different approvals must be submitted before implementation of new software.
V1	Our organization has an efficient Virtual Private Network that users are connected to. Our VPN is an encrypted connection that safely transmits sensitive information/data.	As shown in the Network Diagram in Section 1.3, there is no evidence of encryption for Data at-Rest.	Implementation of encryption for Data at-Rest using symmetric encryption as it is written to storage. Additionally, database backups will be encrypted as well.
V2	Shown in the Network Diagram, there is a Real-Time Malware Detection dedicated server that scans the Local Server live.	There is currently only one Real-Time Malware Detection Server that can be susceptible to external threats.	It should be required that *all databases and servers* have Real-Time Malware Detection to monitor any malicious activity on the machine.
V3	Our network has a low security posture regarding backup databases. As shown in the Network Diagram in Section 1.3, there are no present backups.	Our network does not present a backup of any of the three databases in the diagram. This is a major security concern as these database files can be corrupted, damaged, or changed in the event of an attack.	For the Email, Database, and Application Server backups will be implemented in the Network Design for the upcoming FY. These backups will be a dedicated physical backup machine that will encrypt the data as it is stored.

Isaac Toon

4/22/2023

Principle Assessor **Date**
Isaac S. Yoon

SUMMARY OF REFERENCES

BasuMallick, C. (2022, August 3). *What is an SQL injection? meaning, cheatsheet, examples, and prevention best practices for 2022.* Spiceworks. Retrieved April 22, 2023, from https://www.spiceworks.com/it-security/application-security/articles/what-is-sql-injection/

Georgiev, I. (n.d.). *Bank network infrastructure adopted from (Advanced Relay Corp., 2017 ...* Retrieved April 22, 2023, from https://www.researchgate.net/figure/Bank-Network-Infrastructure-adopted-from-Advanced-Relay-Corp-2017-Cisco-Systems_fig13_324900005

Gibbons, E. (2023, January 27). *What are internal threats in cyber security?* Aspire Technology Solutions. Retrieved April 22, 2023, from https://www.aspirets.com/blog/what-are-internal-threats-cyber-security/

How to audit group policy changes using the Security Event Log. Netwrix. (n.d.). Retrieved April 22, 2023, from https://www.netwrix.com/group_policy_modification_using_logs.html

J.P. Morgan Chase Profile. Street Of Walls. (n.d.). Retrieved April 22, 2023, from https://www.streetofwalls.com/articles/investment-banking/learn-the-basics/j-p-morgan-chase/#:~:text=JP%20Morgan%20Chase%20is%20one,traded%20company%20in%20the%20world.

Kost, E. (n.d.). *Top 8 Cybersecurity Regulations for Financial Services: Upguard.* RSS. Retrieved April 22, 2023, from https://www.upguard.com/blog/cybersecurity-regulations-financial-industry

Martin, A. (2023, January 31). *DDoS attacks rise, a sign of concern for banks, Finance.* Bloomberg.com. Retrieved April 22, 2023, from https://www.bloomberg.com/news/articles/2023-01-31/ddos-attacks-rise-a-sign-of-concern-for-banks-finance#xj4y7vzkg

Namuag, P. (2022, May 4). *Database encryption: Why and where you need to have data encryption.* Severalnines. Retrieved April 22, 2023, from https://severalnines.com/blog/database-encryption-why-and-where-you-need-have-data-encryption/

Naz, Z. (n.d.). *Cybersecurity in banking sector: Importance, threats, challenges.* Cybersecurity in Banking Sector: Importance, Threats, Challenges. Retrieved April 22, 2023, from https://www.knowledgehut.com/blog/security/cyber-security-in-banking

Our business. JPMorgan Chase & Co. (n.d.). Retrieved April 22, 2023, from https://www.jpmorganchase.com/about/our-business

Ozarslan, S. (n.d.). *Key threats and cyber risks facing financial services and banking firms in 2022*. THE COMPLETE SECURITY VALIDATION PLATFORM. Retrieved April 22, 2023, from https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022#:~:text=Ransomware%2C%20phishing%2C%20web%20application%20and,financial%20institutions%20face%20in%202022.

Review of the Department of Health and Human Services' compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020. A-18-20-11200 04-06-2021. (2021, April 6). Retrieved April 22, 2023, from https://oig.hhs.gov/oas/reports/region18/182011200.asp