Facebook Cyber Security Evaluation

Jinnan Sun[1,a*]

[1]Columbia University, School of professional Studies, New York, United States

Abstract. This evaluation is focused on conducting a cybersecurity risk assessment on Facebook, which will map their current practices against the NIST CSF Framework's 4 of the 5 functions. The evaluation will first list the research of Facebook's data breach from public information, then will show the analysis of missing control based on the NIST Framework and provide a logical connection between them.

1. Introduction

1.1 Background

Facebook is an online social media and social networking service owned by Meta Platforms. Facebook has had its fair share of scandals in recent years. The latest one on Facebook's list of problems is "Data Breach" [1].

In 2021, the personal data of more than 530 million Facebook users were made public on online forums and this data was already captured in 2019. Since 2010, Facebook has been frequently found to have security vulnerabilities and data breaches.

1.2 Research aims

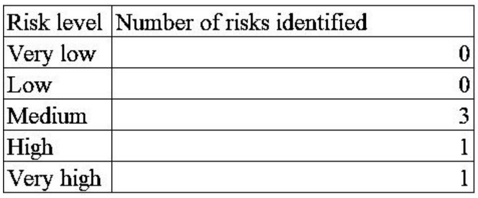
The evaluation will evaluate and assess Facebook's cybersecurity capacities based on **NIST** Framework's 4 functions (Identity, Protect, Detect, Respond) and identify the missing control.

After assessing the cybersecurity capacities, the evaluation will apply the **CMMI** Cybersecurity model to measure Facebook'smaturity and roadmap

1.3 Risk assessment results

The risks will be identified in 5 levels based on the estimation of their impact and likelihood, which forms a **Heat map**. The numbers of risks and their risk levels are listed in the table below:

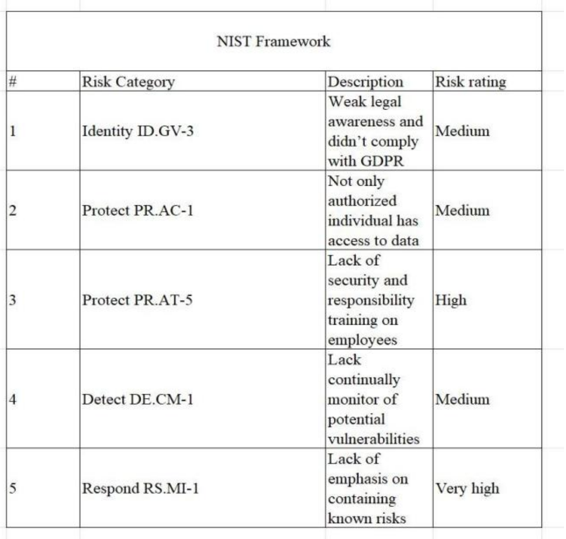
Table 1 risk assessment result self-drawn



Risk level	Number of risks identified
Very low	0
Low	0
Medium	3
High	1
Very high	1

The risk assessment is conducted to identify potential risks associated with the missing NIST Framework functions, which are listed in the below table.

Table 2 NIST Framework functions self-drawn



NIST Framework			
#	Risk Category	Description	Risk rating
1	Identity ID.GV-3	Weak legal awareness and didn't comply with GDPR	Medium
2	Protect PR.AC-1	Not only authorized individual has access to data	Medium
3	Protect PR.AT-5	Lack of security and responsibility training on employees	High
4	Detect DE.CM-1	Lack continually monitor of potential vulnerabilities	Medium
5	Respond RS.MI-1	Lack of emphasis on containing known risks	Very high

CMMI cybersecurity platform:

In this evaluation, after assessing the risks based on NIST Framework, the CMMI cybersecurity platform will be used to identify enterprise risks and prioritize a roadmap for building organizational resilience based on the seven determined missing controls and associated risks evaluating maturity level.

1.4 Literature review

NIST framework has become a hot topic in the recent several years as a high-profile data breach is on the rise. The domestic and foreign academics are relatively active in studying the concept of the NIST framework and how to be used [2]. NIST framework was published to help regulators and industry players identify and mitigate cyber risks. The author Shen Lei mainly talks about three

*Corresponding author: E-mail: 1280538273@qq.com components and four different ways of using the NIST framework in the literature [3]. Barbara Krumay also addressed NIST could be extended to other topic areas, he pointed out that NIST should be engaged more in detecting, responding, and recovering from incidents in his paper [4].

Scholars have analyzed NIST concepts in detail, however, combining the NIST framework with real data breaches and using the CMMI framework to help solve the current situation of enterprises has rarely been studied directly.

2. Risk assessment & recommendation

2.1 Identify

ID. GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed

Facts:

Facebook didn't comply with the GDPR's user privacy policy. So, over 530 million Facebook users' data were posted publicly in August 2021, these data was scraped from Facebook in 2019 [5]. However, it didn't notify these users about this scrap of personal data as it fixed the vulnerability by Sep 2019.

Risks:

Facebook's legal awareness is weak.

Facebook will be fined for violating the laws of different areas and causing serious social impact and reputation damage.

Recommendations:

Facebook should be in contact with lawyers in different regions (especially in the US and Europe) to meet the legal requirements.

Stay on top of regulatory changes and be proactive about checking the updated standards and regulations.

Ensure that company policies and procedures are properly documented. That non-compliance is continuously monitored and corrected through the company's legal department, such as making sure the legal professionals work with compliance officers.

Risk level: Median Likelihood: Remote Impact: Catastrophic

2.2 Protect

PR. AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes

Facts:

Facebook doesn't pay attention to the restrictions on employee data access and misses the proper identification and access control to prevent unauthorized individuals from viewing and posting internal information.

Risks:

Third-party developers could view and change the data that they aren't entitled to access.

The internal information would be exposed to the public and hard to track who revealed it.

Recommendations:

The "CIA" of security should be strictly observed. Facebook should ensure that only authorized individuals could be able to access these data and create or change this information.

Facebook should develop a new system to monitor and report the authorized access control, and also should audit the authorized individuals' accounts regularly.

Risk level: Median Likelihood: Occasional Impact: Significant

2.3 Protect

PR. AT-5: Physical and cybersecurity personnel understand their roles and responsibilities

Facts:

These Facebook developers have not gone through rigorous training to make it clear to them that user data should be stored on internal, non-public servers. As a result, about 540 million users' records were captured by Facebook developers and stored in an Amazon public cloudpublic server in 2019.

Risks:

The developers didn't truly understand cybersecurity people's responsibilities. They would be attacked easily (such as phishing attacks) and more internal data would be revealed through their wrong operation.

Recommendations:

Instill the corporate culture and educate employees on cybersecurity before they start their work. Make them clearly understand the serious consequences if they fail to maintain cybersecurity.

Regularly hold relevant training on cybersecurity, through the training to inculcate the importance of cybersecurity and how to achieve it.

Risk level: High Likelihood: Probable Impact: Significant

2.4Detect

DE.CM-1: The network is monitored to detect potential cybersecurity events.

Facts:

Facebook does not continuously monitor for potential cybersecurity vulnerabilities, resulting in vulnerabilities that arise going undetected promptly. So, an internal glitch in the Facebook system prevented the privacy settings from working, so the private posts of more than 14 million users were publicly revealed in 2018.

Risks:

The vulnerability becomes large and affects other operations, causing a major impact on the entire system and leading to disruptions of operations.

Recommendations:

Keep testing the vulnerabilities within the system, hold the internal stress test of it and produce a continuity plan.

Develop a monitoring system to continuously monitor the vulnerabilities

Document these vulnerabilities in detail and report to specialists who're responsible to solve this cyber trouble and try to avoid this in the future

Risk level: Median

Likelihood: Remote Impact: Catastrophic

2.5 Respond

RS.MI-1: Incidents are contained.

Facts:

Most vulnerabilities identified in Facebook were not mitigated. From 2007, when Facebook first encountered massive privacy problems, to the present day, frequent user privacy attacks have shown that Facebook does not contain themseriously.

Risks:

Cyber vulnerabilities and potential risks will increase. It may be more difficult to deal with therisk afterward

Users lose confidence in Facebook and think Facebook is a company full of lies

Recommendations:

Use monitoring tools and analysis tools to screen and organize network security vulnerabilities, set up specialists or automated systems to help resolve vulnerabilities, and detailed records to avoid recurrence

Facebook could use Archer to analyze operating risks, and input the questionnaires on the platform and these questionnaires would be recorded

Risk level: Very high Likelihood: Frequent Impact: Catastrophic

3. CMMI level analyze

3.1 CMMI's current level & target level

Based on the above five determined missing controls and associated risks, the CMMI Maturity level is measured in seven areas: ensure governance framework, establish risk management, identify and manage risks, ensure risk mitigation, ensure risk mitigation, ensure risk detection, ensure risk exposure, and ensure resilience.

The CMMI Maturity level is scored by the CMMI Scoring methodology in five levels, which are shown in the histogram below:

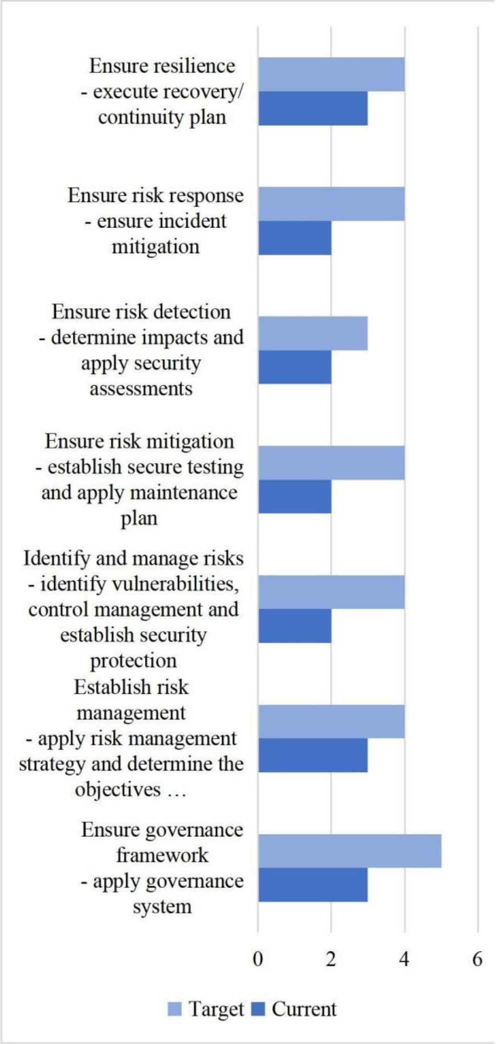


Figure 1: Histogram self-drawn

4. Conclusion

The cybersecurity risk in Facebook can be successfully assessed by the NIST framework was clearly expressed. CMMI model was combined with the NIST framework to address Facebook's current management weaknesses on five levels. Future work will investigate how to use CMMI's road map to formulate specific actions to solve management problems in different stages in an orderly manner, and how to use other frameworks to analyze other important risks within Facebook, such as market risk and financial risk.

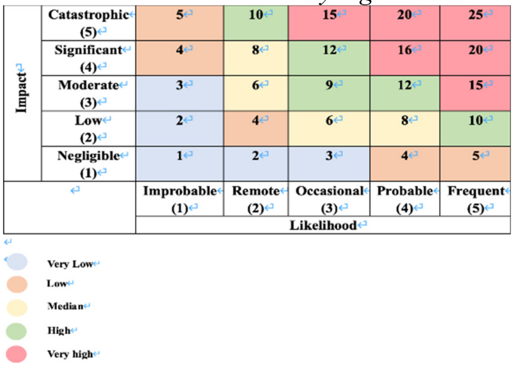
5. Appendix

5.1 What is Archer

RSA Archer Suite is a risk management platform that provides solutions in enterprise operational risk management. Archer suites risk data from organizations and outputs risk analytics to provide an integrated risk report. These reports can help enterprises document the known risks and try to avoid them.

5.2 Heat map

This risk heat map offers data visualization for assessing the risks in Facebook through quantifying likelihood and impact. Risks are divided into five severity levels according to the depth of the color, the lightest cells represent the risk level is *very low*, and the darkest is *very high*.



Impact						
	Catastrophic (5)	5 🟧	10 🟩	15 🟥	20 🟥	25 🟥
	Significant (4)	4 🟧	8 🟨	12 🟩	16 🟥	20 🟥
	Moderate (3)	3 🟦	6 🟨	9 🟩	12 🟩	15 🟥
	Low (2)	2 🟦	4 🟧	6 🟨	8 🟨	10 🟩
	Negligible (1)	1 🟦	2 🟦	3 🟦	4 🟧	5 🟧
		Improbable (1)	Remote (2)	Occasional (3)	Probable (4)	Frequent (5)
		Likelihood				

🟦 Very Low
🟧 Low
🟨 Median
🟩 High
🟥 Very high

Figure 2 heat map self-drawn

5.3 What is "CIA"

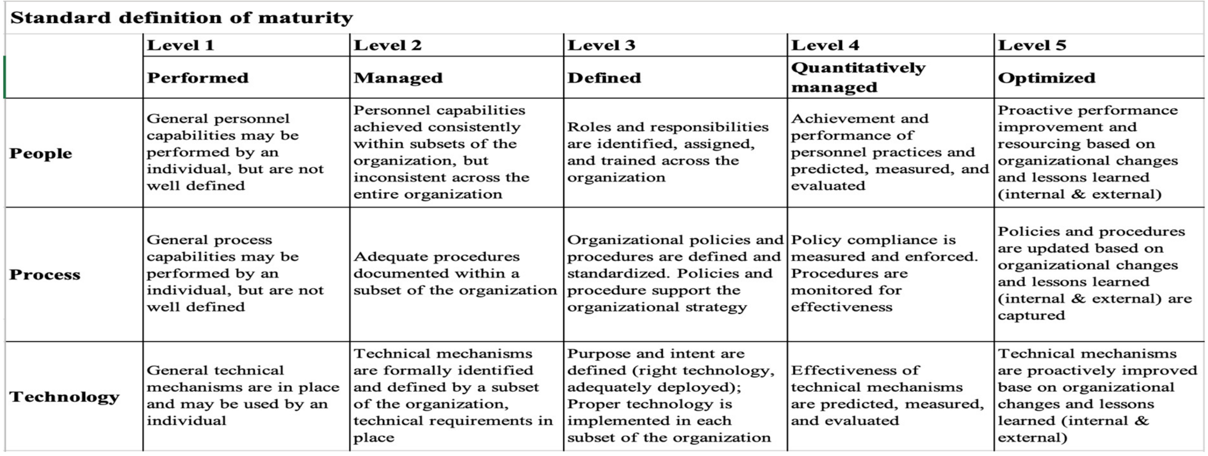
The CIA of security.

C is confidentiality, to ensure that only authorized individuals could view information

It is integrity, only authorized people could create and change information

A is availability, to ensure that the data and system are available when authorized people want it.

5.4 CMMI scoring methodology



Standard definition of maturity					
	Level 1	Level 2	Level 3	Level 4	Level 5
	Performed	Managed	Defined	Quantitatively managed	Optimized
People	General personnel capabilities may be performed by an individual, but are not well defined	Personnel capabilities achieved consistently within subsets of the organization, but inconsistent across the entire organization	Roles and responsibilities are identified, assigned, and trained across the organization	Achievement and performance of personnel practices and predicted, measured, and evaluated	Proactive performance improvement and resourcing based on organizational changes and lessons learned (internal & external)
Process	General process capabilities may be performed by an individual, but are not well defined	Adequate procedures documented within a subset of the organization	Organizational policies and procedures are defined and standardized. Policies and procedure support the organizational strategy	Policy compliance is measured and enforced. Procedures are monitored for effectiveness	Policies and procedures are updated based on organizational changes and lessons learned (internal & external) are captured
Technology	General technical mechanisms are in place and may be used by an individual	Technical mechanisms are formally identified and defined by a subset of the organization, technical requirements in place	Purpose and intent are defined (right technology, adequately deployed); Proper technology is implemented in each subset of the organization	Effectiveness of technical mechanisms are predicted, measured, and evaluated	Technical mechanisms are proactively improved base on organizational changes and lessons learned (internal & external)

Figure 3 CMMI scoring methodology self-drawn

References

1. Franklin D. Azar & Associates, P.C. (2022) Facebook (Data Breach) Retrieved August 8, 2022, from https://www.fdazar.com/practice-areas/class-action/facebook-data-breach/.
2. Heiligenstein, M. X., Jodi, Robert, & Smith, O. (2022, March 21) Facebook data breaches: Full timeline through 2022. Firewall Times.
3. Shen, Lei. (2014) The nist cybersecurity framework: overview and potential impacts. J. Scitech Lawyer, 10(4): 16-19.
4. Krumay, B., Bernroider, E. W., & Walser, R. (2018) Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST Cybersecurity Framework. J. Secure IT Systems, 369–384.
5. Holmes, A. (2021). 533 million Facebook users' phone numbers and personal data have been leaked online. J. Business Insider.