|  |
| --- |
| RMA’s 2022 Carolinas Virginias Spring Conference  Risk Assessment Report |
| RA3 |



**CIS 650 – RA3**

**Utsav Khatiwada**

Contents

[1](#_Toc118665478)

[Overview: 3](#_Toc118665479)

[Problem: 3](#_Toc118665480)

[Scenario 1: C1 (united community bank): 3](#_Toc118665481)

[Attacks happened before in the united community bank 4](#_Toc118665482)

[Fair-U tool risk analysis: 5](#_Toc118665483)

[Scenario 2: C2 (Wells Fargo Bank): 6](#_Toc118665484)

[Attacks happened before in the Wells Fargo bank: 6](#_Toc118665485)

[FairU tool risk analysis C2(Wells Fargo) 7](#_Toc118665486)

[Control Measures: 8](#_Toc118665487)

[Delete leaked information: 8](#_Toc118665488)

[Insurance: 8](#_Toc118665489)

[References: 9](#_Toc118665490)

# Overview:

In the given scenario the RMA group of an organization is a group of organization of risk managers. The members of that organization work with prestigious companies, including Bank of America Merrill Lynch, Barclays, Blackrock, BNP Paribas, Credit Suisse, and many more recognizable names. During RMA’s 2022 Carolinas Virginias Spring Conference which took place in April 2022, the conference posted the list of attendees including first names, last names, and the company they worked for. This release of the name of risk managers created a problem. Since Risk managers do not like to be in the spotlight as they routinely explore the most sensitive areas of their respective organizations. They know all the secrets. They have to, that’s their role. So, this risk management report will be including a risk assessment of the impact of this release on the people whose names have been exposed.

# Problem:

The problem in the current scenario is related to the risk managers. As in the scenario the list of risk managers’ names has been released publicly, which will negatively impact the respective organization they are involved with. As risk managers are supposed to know all the secrets of their organization, once their name is released attacker can focus their attacks on risk managers, in case they get successful, they will have the ability to compromise the data that the risk managers have authority on.

Data inputs for primary loss:

|  |  |  |  |
| --- | --- | --- | --- |
| Inputs | Minimum | Most Likely | Maximum |
| Reputation | 6000000 | 8000000 | 10,000,000 |

Data inputs for Secondary loss:

|  |  |  |  |
| --- | --- | --- | --- |
| Inputs | Minimum | Most Likely | Maximum |
| Reputation | 50000000 | 70000000 | 100000000 |

The above values are assumed according to the data provided with the reputational damage faced with high confidence. The primary loss starts from 6-10 million. The secondary values are based on the attacker’s successful attacks on protected data which leads to damage from 50-100 million

# Scenario 1: C1 (united community bank):

United community bank serves businesses and individuals in small geographic areas. They believe in combining top-of-manager financial solutions with award-winning satisfaction for our customers. Recently in RMA’s 2022 Carolinas Virginias Spring Conference, the united community bank risk manager’s name has been exposed publicly, following a risk analysis report made for the impact of the ease.

# Attacks happened before in the united community bank

According to bizjournal.com United community bank has faced cyber breaches in recent years. Attackers attacked the North Carolina government payroll which cost them around $460000. They got $250000 from the insurance and united community bank had to settle it by giving an additional $180000. This information shows the vulnerability of the cyber security of the bank. In contrast to the current scenario, the leaked name of the risk manager of united community bank will create a huge impact. When the attacker knows the name of the risk manager his target choice will be straight to one person. There will be multiple attacks on a single person. the chance of attackers’ strength will enhance directly. If the attacker attempts to target a single person with different attacking methods a minimum of 1 time a day, the chances of getting victimized will rise. Moreover, if the attacker gets successful to get to the risk manager device or network. They can compromise the data which will destruction of the company(Bizjournals.com).

Text

Description automatically generated

Threat event frequency is determined by the previous attacks that the united community has faced. If the name of the risk manager is exposed to hackers, then the number of times the attack is done by the attacker is assumed to be at least 1 per day with a maximum of 3 per day. Which leads to be 365 to 1000 attacks annually.

Text

Description automatically generated

When the risk managers’ names have been exposed the chances of getting attacks are increased. The reason behind this is the attackers get a direct option to the target. They do not have to filter out whom to attack as their target is already specified with the name. They can use different tools or even can-do social engineering attacks or they can impersonate by using the risk manager’s name.

Text

Description automatically generated

The resistance strength is based on the new security solution that the united bank has come up with after their previous attacks. They have implemented unique Id login and secured software for transferring data. Moreover, they have implemented Id authentication to prevent from social engineering attacks(United Community Bank).

# Graphical user interface Description automatically generatedTable Description automatically generatedDiagram Description automatically generated with medium confidenceFair-U tool risk analysis:

The above figure represents the risk analysis report result of the impact of the release of the risk manager name of a united community bank. The analysis results are based on threat event frequency, threat capability, and resistance strength. This result is based on the successfulness of attack due to the release of the name of the risk manager where the minimum loss is going to be 3.2B to a maximum of 13.6 B according to the loss exceedance curve. It shows if a 2-8% of chance of secondary loss due to attack is successful then the secondary loss is more destructive than the primary loss. Due to the release of the name the vulnerability of united community bank has gone up to 87.08% which can severely impact the bank as well as the risk manager personally.

# Scenario 2: C2 (Wells Fargo Bank):

Recently in RMA’s 2022 Carolinas Virginias Spring Conference, the Wells Fargo bank risk manager’s name has been exposed publicly, following a risk analysis report made for the impact of the ease.

# Attacks happened before in the Wells Fargo bank:

There have been a lot of data breaches happening in Wells Fargo in previous years. One of the data breaches occurred in 2016/2017 year. Within the year the employees of Wells Fargo bank had opened several fake accounts without the customer’s permission. It was estimated that around 2.1 million fake accounts were created. This leads them to lose 6.1 million dollars for refunding the customer (U.S News).

Threat event frequency is determined by the previous attacks that the united community has faced. If the name of the risk manager is exposed to hackers, then the number of times the attack is done by the attacker is assumed to be at least 1 per day with a maximum of 3 per day. Which leads to be 365 to 1000 attacks annually.

Text

Description automatically generated

When the risk managers’ names have been exposed the chances of getting attacks are increased. The reason behind this is the attackers get a direct option to the target. They do not have to filter out whom to attack as their target is already specified with the name. They can use different tools or even can-do social engineering attacks, or they can impersonate by using the risk manager’s name.

Graphical user interface, text, chat or text message

Description automatically generated

The resistance strength is based on the new security solution that Wells Fargo has come up with after their previous attacks. They have implemented. Since Wells Fargo is a large company with big monetary values its security strength is still strong enough to hold from huge loss to the company, therefore their resistance strength is still good.

Graphical user interface, text, application

Description automatically generated

# A picture containing chart Description automatically generatedGraphical user interface, table Description automatically generatedF**airU tool risk analysis C2(Wells Fargo)**

A picture containing diagram

Description automatically generated

The above figure represents the risk analysis report result of the impact of the release of the risk manager name of a Wells Fargo bank. The analysis results are based on threat event frequency, threat capability, and resistance strength. This result is based on the successfulness of attack due to the release of the name of the risk manager where the minimum loss is going to be 1.9B to a maximum of 7.8 B according to the loss exceedance curve. It shows if a 2-8% of chance of secondary loss due to attack is successful then the secondary loss is more destructive than the primary loss. Due to the release of the name the vulnerability of Wells Fargo bank has shown up to 51.99%.

# Control Measures:

## Delete leaked information:

In this case, RMA should try to delete released names from the third party and websites, newspapers, and magazines as soon as possible. Moreover, they need to assemble a team of experts to conduct a comprehensive breach response.

## Insurance:

RMA should purchase insurance in hand for upcoming cases. Sometimes there might be human error that can lead to leakage of the information. In this case, to reduce the loss for the company, good insurance should be purchased to reduce the loss for the company in such data breach cases.

# References:

Bizjournals.com. (n.d.). Retrieved November 6, 2022, from https://www.bizjournals.com/atlanta/news/2020/12/08/cyber-thieves-459-000-united-community-bank.html

*Security statement*. United Community Bank. (n.d.). Retrieved November 6, 2022, from https://www.ucbi.com/security-statement/

*Wells Fargo: More Than 3M possibly fake accounts created*. (n.d.). Retrieved November 7, 2022, from https://www.usnews.com/news/national-news/articles/2017-08-31/wells-fargo-estimates-35-million-accounts-impacted-by-scandal