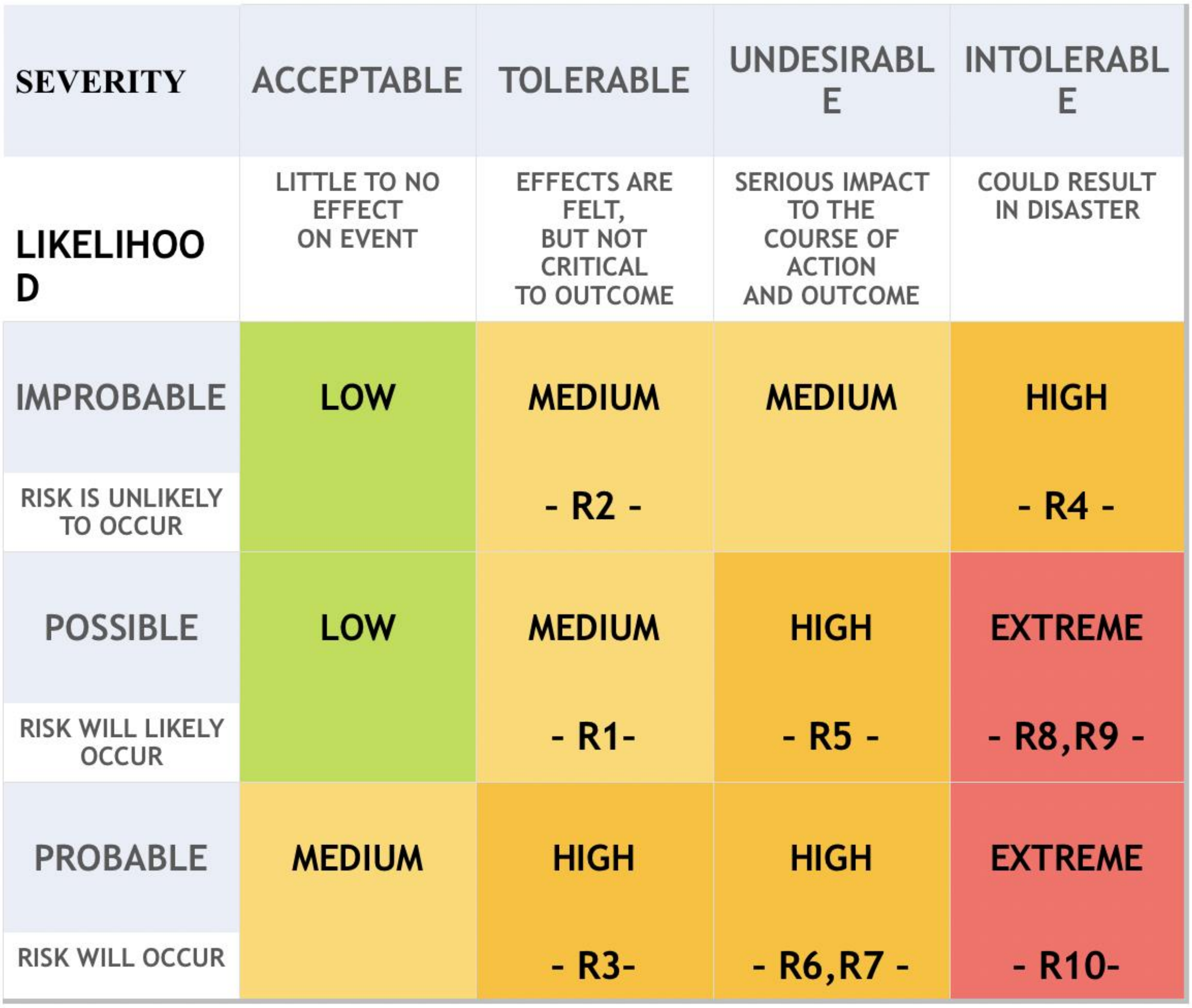
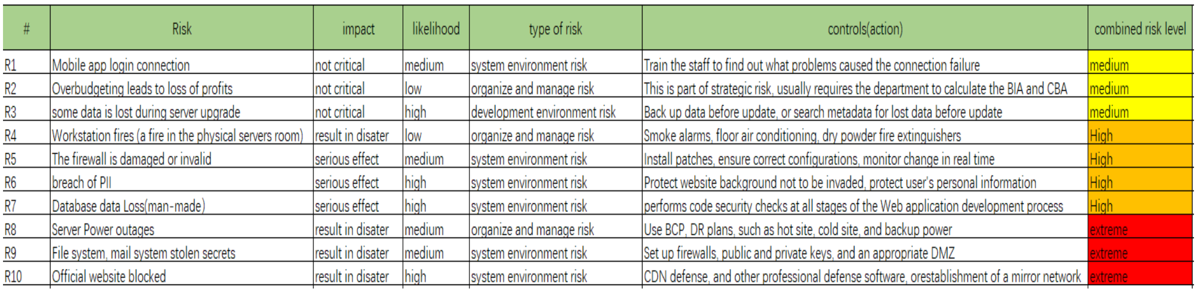
ISMN5740-TMX bank case
Bojun zhang
10.26

1.Qualitative Assessment

The following is qualitative analysis, which usually starts with qualitative analysis, which can help the management or clients focus on some risks, understand why these risks occur, the possibility of occurrence, and the negative impact. Among them, the risk category includes system environment risk, development environment risk, organize and manage risk. Among them, the main risks are from the system and technical level, but also mentioned from the physical level and administrative level of risk. The table below categorizes each risk by impact and explains the causes of the risk and how to mitigate the impact of the risk.



SEVERITY	ACCEPTABLE	TOLERABLE	UNDESIRABLE	INTOLERABLE
LIKELIHOOD	LITTLE TO NO EFFECT ON EVENT	EFFECTS ARE FELT, BUT NOT CRITICAL TO OUTCOME	SERIOUS IMPACT TO THE COURSE OF ACTION AND OUTCOME	COULD RESULT IN DISASTER
IMPROBABLE RISK IS UNLIKELY TO OCCUR	LOW	MEDIUM - R2 -	MEDIUM	HIGH - R4 -
POSSIBLE RISK WILL LIKELY OCCUR	LOW	MEDIUM - R1-	HIGH - R5 -	EXTREME - R8,R9 -
PROBABLE RISK WILL OCCUR	MEDIUM	HIGH - R3-	HIGH - R6,R7 -	EXTREME - R10-



#	Risk	impact	likelihood	type of risk	controls(action)	combined risk level
R1	Mobile app login connection	not critical	medium	system environment risk	Train the staff to find out what problems caused the connection failure	medium
R2	Overbudgeting leads to loss of profits	not critical	low	organize and manage risk	This is part of strategic risk, usually requires the department to calculate the BIA and CBA	medium
R3	some data is lost during server upgrade	not critical	high	development environment risk	Back up data before update, or search metadata for lost data before update	medium
R4	Workstation fires (a fire in the physical servers room)	result in disater	low	organize and manage risk	Smoke alarms, floor air conditioning, dry powder fire extinguishers	High
R5	The firewall is damaged or invalid	serious effect	medium	system environment risk	Install patches, ensure correct configurations, monitor change in real time	High
R6	breach of PII	serious effect	high	system environment risk	Protect website background not to be invaded, protect user's personal information	High
R7	Database data Loss(man-made)	serious effect	high	system environment risk	performs code security checks at all stages of the Web application development process	High
R8	Server Power outages	result in disater	medium	organize and manage risk	Use BCP, DR plans, such as hot site, cold site, and backup power	extreme
R9	File system, mail system stolen secrets	result in disater	medium	system environment risk	Set up firewalls, public and private keys, and an appropriate DMZ	extreme
R10	Official website blocked	result in disater	high	system environment risk	CDN defense, and other professional defense software, orestablishment of a mirror network	extreme

Risk description:

R1- Mobile app login connection

Mobile banking software network connection problems, such as many mobile applications often appear network fluctuations, resulting in login failure, or data cannot be updated in time. Such risks could reduce customer satisfaction at TMX Bank.

R2-overbudgeting leads to loss of profits

This is a strategic issue and has little to do with system security. This is mainly in the early deployment, such as TMX Bank's purchase of banking App Suite, Transaction Processing Server and other equipment. Or implement various controls to reduce the cost of loss. This kind of risk mainly requires the department to calculate BIA, CBA, and compare various costs with the profits they bring.

R3-data is lost during server upgrade

This usually occurs during a system upgrade or server upgrade, and it is possible that data or default Settings will be lost during the upgrade.

R4-workstation fires

This generally refers to the security of physical servers or other devices. There may be a fire in the server room due to high temperature or machine aging, or the TELLER Terminal machine of TMX may be damaged due to natural or human factors. As a result, the company can not operate normally, and huge losses.

R5-the firewall is damaged or invalid

Firewalls are a fundamental part of any company's network security architecture. There are five common risks, such as Insider Attacks, Missed Security Patches, Configuration Mistakes, A Lack of Deep Packet Inspection, DDoS Attacks, which can cause firewalls to fail to secure internal software or servers.

R6-breach of PII

A breach may also include the loss or theft of physical documents that include PII or portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website. A customer-focused company like TMXbank should protect the privacy of its customers.

R7-Database data loss(man-made)

This refers to malicious theft of data from a database, or data in the background of a web page.

Generally more common have SQL injection, crawler. Some hackers use technology to steal confidential data, which leads to the disclosure of users' and companies' private information. And through the operation of the database, tamper with the database of specific web pages, directly resulting in profit loss.

R8-server power outages
This refers to an unexpected situation, usually a natural disaster that causes a power outage and prevents servers or other company facilities from functioning properly.

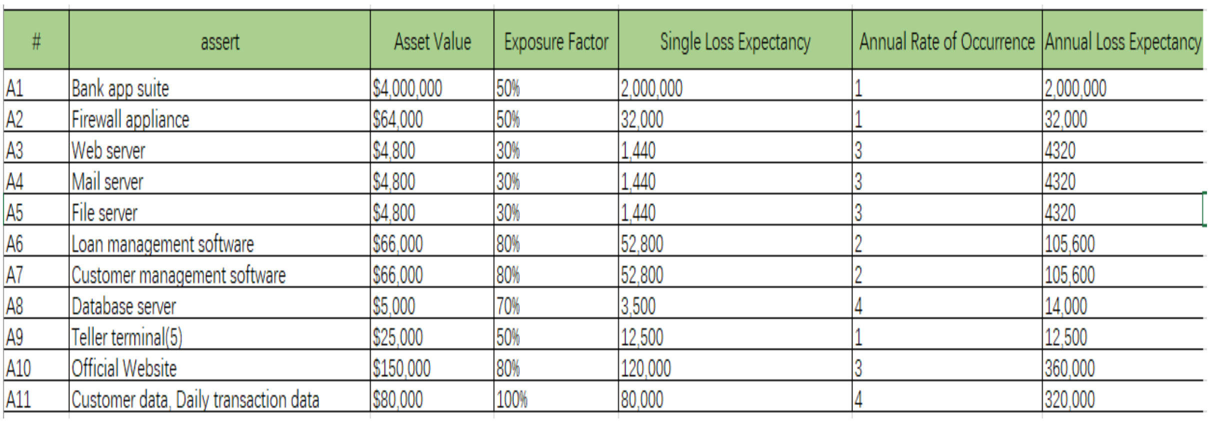
R9-file system, mail system stolen secrets
Hackers use technical means to attack firewalls and gain control authority. For example, an buffer overflow attack can steal confidential emails, specific files and so on.

R10-official website blocked
The risk can be divided into two situations. The first is that the server responds slowly due to heavy customer traffic. Another is malicious attacks by hackers, who use DOS or DDOS technology to attack the website of TMXbank, leading to the direct failure of the website. Every hour that the official website is blocked takes a huge toll.

2.Quantitative Assessment

Quantitative analysis is mainly divided into the following aspects:
first, Asset value (AV) refers to the value of resources to the organization. The value of these assets comes from the Asset register.
The second is Exposure Factor, The exposure factor (EF) is the percentage of asset loss caused by a successful threat attack. For example, when an asset is subjected to a physical or technical attack, it is generally not completely damaged, but still has data value or value after the danger has passed.
The third is single expected loss (SLE) is the amount of money expected to be lost from any successful threat attack on any given asset. This is the monetary value of how much damage an accident would cause in terms of asset value losses.
The fourth one is Annual occurrence rate, The annualized occurrence rate (ARO) determines the frequency of successful threat attacks within a year.
The last one is Annual Loss Expected. ALE=SLE X ARO.
Annual loss expected (ALE) estimates the annual loss caused by the event.

As for the quantitative risk analysis, I think there are certain limitations if only the qualitative analysis in the table above is used, because the qualitative analysis only describes the risks that TMXbank is most likely to face. Similarly, other companies also have such risks, because each company has different system scale, data scale and protective measures. So I use asset Register to calculate the cost of each component, system, or physical device. Finally, one or more of them are combined with the risks in the qualitative risks to determine the possible loss of each risk.



#	assert	Asset Value	Exposure Factor	Single Loss Expectancy	Annual Rate of Occurrence	Annual Loss Expectancy
A1	Bank app suite	$4,000,000	50%	2,000,000	1	2,000,000
A2	Firewall appliance	$64,000	50%	32,000	1	32,000
A3	Web server	$4,800	30%	1,440	3	4320
A4	Mail server	$4,800	30%	1,440	3	4320
A5	File server	$4,800	30%	1,440	3	4320
A6	Loan management software	$66,000	80%	52,800	2	105,600
A7	Customer management software	$66,000	80%	52,800	2	105,600
A8	Database server	$5,000	70%	3,500	4	14,000
A9	Teller terminal(5)	$25,000	50%	12,500	1	12,500
A10	Official Website	$150,000	80%	120,000	3	360,000
A11	Customer data, Daily transaction data	$80,000	100%	80,000	4	320,000

explanation for each of the above figures:
There are fixed assets that come from a given data set,
Database Server, which is based on the value of the other three servers
Teller Terminal, value from online query
Official website, from the source the value of the mirror network is 64000, all estimates of the official website value is 150000
The value of Customer data and Dail Data from data backup is 64,000, and the estimated value of company data is about 80,000

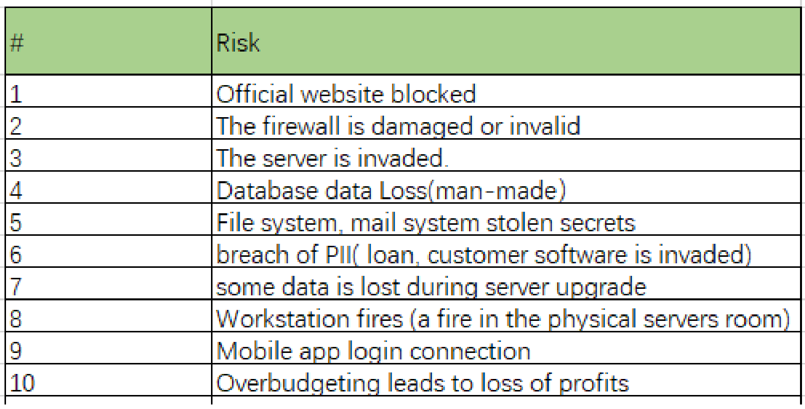
In terms of Exposure factor, most of it is based on estimates. I have Exposure factor around 50% or less for assets such as servers or firewall systems, because the system can still function after an attack, but it just needs to reset default Settings and re-import data, etc. For Loan Management Software and Customer Management Software, I think the Exposure factor is on the high side, because it involves not only the privacy of the company, but also the privacy of customers and a series of data. As for the Exposure factor of the official website, I think it is also about 80%. After the website is attacked, it will lose a lot of information and data, and customers will not be able to log in normally, or even be cheated. Finally, customer data and transaction data, WHICH I would say is as high as 100%, because once the system is breached, all the valuable data is stolen.

I usually set the Annual rate of occurrence to occur once a year, but I think the dangerous times of website attacks and database attacks will be more frequent.

3.Prioritize Risk Register

The following table is a comprehensive analysis of qualitative and quantitative analysis of the 10 risks, the severity from top to bottom.
Firstly, official website blocked. TMXbank is a customer-oriented bank, so every hour of network congestion may bring huge losses. In terms of hacker attacks, cross-site attacks are the second largest means of network technical attacks.
The second is firewall, in which TMXbank invested a lot of money, and firewall is the only means to protect the company's internal, so it ranks the second.
The third one is server breakdown. TMXbank has many servers, such as mail, file and database servers.

If any of these servers stops working, the normal operation of the company will be affected.
Number four, five, and six are all about data theft, database attacks, and the dangers of customer privacy. As SQL injection is the most common attack at present, I put database Data Loss in the first place, and sorted the remaining two according to the amount of loss.
Seventh, the loss of data is unexpected, but it can still cause some damage
Eighth, ninth, and tenth in terms of physical hazards and decision hazards, not so much in terms of system hazards, I ranked them by the amount of damage that was quantitatively analyzed.



#	Risk
1	Official website blocked
2	The firewall is damaged or invalid
3	The server is invaded.
4	Database data Loss(man-made)
5	File system, mail system stolen secrets
6	breach of PII(loan, customer software is invaded)
7	some data is lost during server upgrade
8	Workstation fires (a fire in the physical servers room)
9	Mobile app login connection
10	Overbudgeting leads to loss of profits

Reference

Eric Dosal, 2018/04/12, 5 Firewall Threats and Vulnerabilities to Look Out For, from(www.compuquip.com)

How to protect yourself against hackers. (n.d.). Retrieved April 26, 2021, from https://www.ag.state.mn.us/consumer/publications/HowtoProtectYourselfAgainstHackers.asp

Personally Identifiable Information (PII): Breaches. U.S.ARMY, from https://www.rmda.army.mil/privacy/PII/PII-breaches.html

ChipsDie, 2020-09-14, HOW to Defend against SQL injection Attacks, from https://www.php.cn/faq/419041.html

Effective solution to web site network blocked, 2018/01/16, from https://jingyan.baidu.com/article/fec7a1e5c5261d1190b4e7f7.html

How Much Should a Website Cost in 2021?, from https://www.webfx.com/How-much-should-web-site-cost.html

BAOYU ZHANG, In the era of big data, how much is corporate data worth, 2016/09/28,from http://qnck.cyol.com/html/2016-09/28/nw.D110000qnck_20160928_1-14.htm