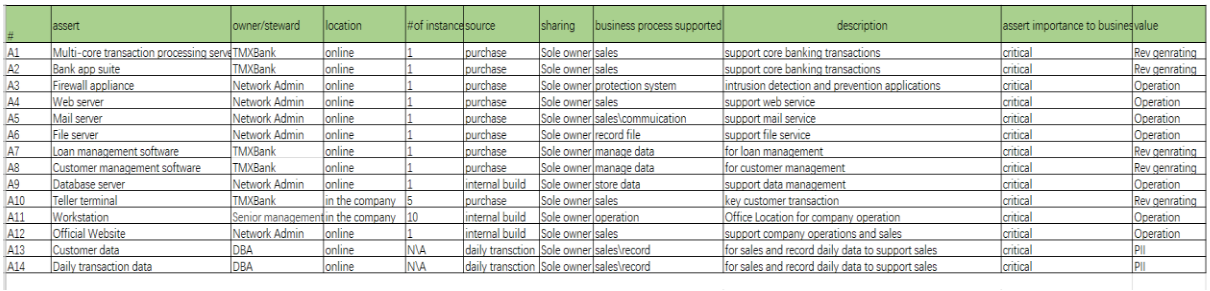
1. Asset Register & Discussion

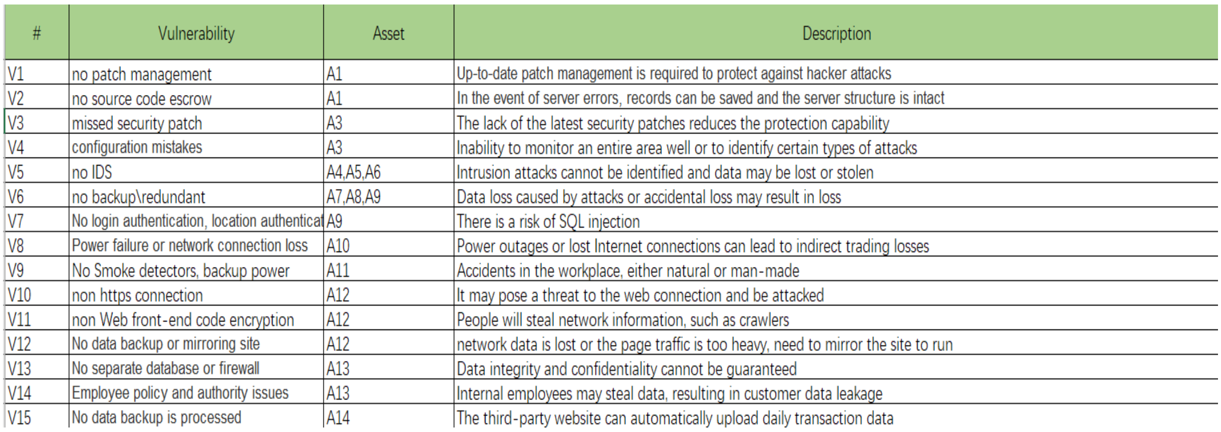
For the asset register below, the different assets owned or managed by TMXBank are described in detail. The main assets are systems, servers and trading procedures (A1-A10), which are owned by TMXBank and some specific managers. The main function of each asset is to support sales and the main business operation of the company. Note that the server may be in the form of a physical server or a cloud server. In the table below, the network security aspect of the server is mainly targeted rather than the physical security aspect, so the location belongs to the 'online'. As well as some intangible assets, such as customer data, transaction data, etc., are mentioned as important factors in the table below.This asset register allows companies to track and record complete details of assets. It is convenient for the company to reference when making a decision.



#	assert	owner/steward	location	#of instance	source	sharing	business process supported	description	assert importance to busines	value
A1	Multi-core transaction processing serve	TMXBank	online	1	purchase	Sole owner	sales	support core banking transactions	critical	Rev genrating
A2	Bank app suite	TMXBank	online	1	purchase	Sole owner	sales	support core banking transactions	critical	Rev genrating
A3	Firewall appliance	Network Admin	online	1	purchase	Sole owner	protection system	intrusion detection and prevention applications	critical	Operation
A4	Web server	Network Admin	online	1	purchase	Sole owner	sales	support web service	critical	Operation
A5	Mail server	Network Admin	online	1	purchase	Sole owner	sales\commuication	support mail service	critical	Operation
A6	File server	Network Admin	online	1	purchase	Sole owner	record file	support file service	critical	Operation
A7	Loan management software	TMXBank	online	1	purchase	Sole owner	manage data	for loan management	critical	Rev genrating
A8	Customer management software	TMXBank	online	1	purchase	Sole owner	manage data	for customer management	critical	Rev genrating
A9	Database server	Network Admin	online	1	internal build	Sole owner	store data	support data management	critical	Operation
A10	Teller terminal	TMXBank	in the company	5	purchase	Sole owner	sales	key customer transaction	critical	Rev genrating
A11	Workstation	Senior management	in the company	10	internal build	Sole owner	operation	Office Location for company operation	critical	Operation
A12	Official Website	Network Admin	online	1	internal build	Sole owner	sales	support company operations and sales	critical	Operation
A13	Customer data	DBA	online	N\A	daily transction	Sole owner	sales\record	for sales and record daily data to support sales	critical	PII
A14	Daily transaction data	DBA	online	N\A	daily transction	Sole owner	sales\record	for sales and record daily data to support sales	critical	PII

2. Vulnerability registration & discussion

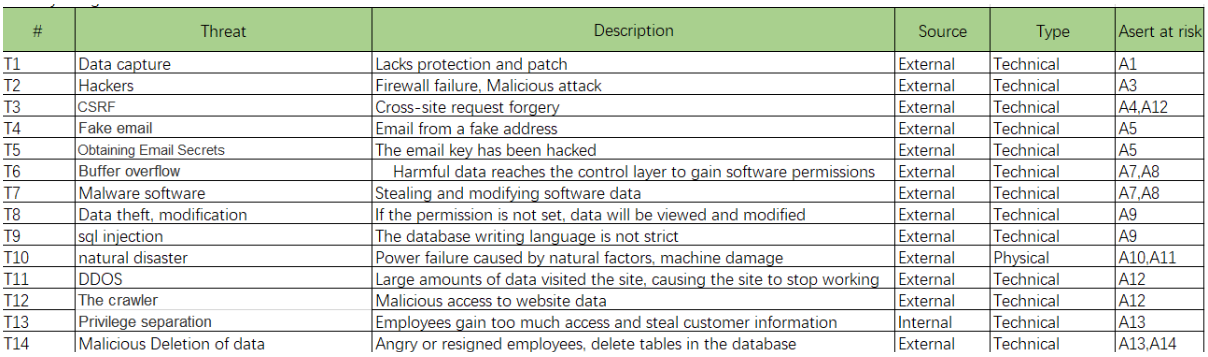
In the vulnerability register is the weakness of the asset. This includes reducing controls and costs. We can use it to classify assets and functions in the system. The main part of attention is network security, many network security vulnerabilities for attackers to build Bridges, so the following installation of firewalls, update patches, modify the default Settings, etc., can play an effective defense. Secondly, data loss, network connection loss and website connection loss caused by natural factors or other factors are all mentioned below. This allows managers to understand vulnerabilities and protect them accordingly.



#	Vulnerability	Asset	Description
V1	no patch management	A1	Up-to-date patch management is required to protect against hacker attacks
V2	no source code escrow	A1	In the event of server errors, records can be saved and the server structure is intact
V3	missed security patch	A3	The lack of the latest security patches reduces the protection capability
V4	configuration mistakes	A3	Inability to monitor an entire area well or to identify certain types of attacks
V5	no IDS	A4,A5,A6	Intrusion attacks cannot be identified and data may be lost or stolen
V6	no backup\redundant	A7,A8,A9	Data loss caused by attacks or accidental loss may result in loss
V7	No login authentication, location authenticat	A9	There is a risk of SQL injection
V8	Power failure or network connection loss	A10	Power outages or lost Internet connections can lead to indirect trading losses
V9	No Smoke detectors, backup power	A11	Accidents in the workplace, either natural or man-made
V10	non https connection	A12	It may pose a threat to the web connection and be attacked
V11	non Web front-end code encryption	A12	People will steal network information, such as crawlers
V12	No data backup or mirroring site	A12	network data is lost or the page traffic is too heavy, need to mirror the site to run
V13	No separate database or firewall	A13	Data integrity and confidentiality cannot be guaranteed
V14	Employee policy and authority issues	A13	Internal employees may steal data, resulting in customer data leakage
V15	No data backup is processed	A14	The third-party website can automatically upload daily transaction data

3. Threat registration & discussion

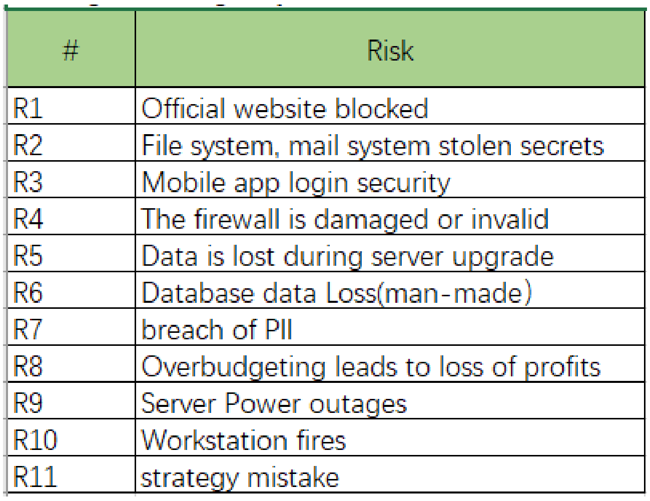
A threat is any activity of an asset that may pose a risk. In the Threat register, it contains the description and control for each threat. This is an important step in risk assessment, some of it natural, some of it artificial. Such as email encryption, cross-site requests (connections from a secure site to a compromised site), SQL injection are the most common threats to databases that can lead to data leakage and modification. The following is a list of well-known cyber attacks that require professionals to solve. At the same time, physical threats can also cause huge losses, A workplace shutdown or a website shutdown is directly related to loss, so according to the situation to do hot site, cold site, data backup, is also very important. Using this information can reasonably and effectively realize network security and security design.



#	Threat	Description	Source	Type	Asert at risk
T1	Data capture	Lacks protection and patch	External	Technical	A1
T2	Hackers	Firewall failure, Malicious attack	External	Technical	A3
T3	CSRF	Cross-site request forgery	External	Technical	A4,A12
T4	Fake email	Email from a fake address	External	Technical	A5
T5	Obtaining Email Secrets	The email key has been hacked	External	Technical	A5
T6	Buffer overflow	Harmful data reaches the control layer to gain software permissions	External	Technical	A7,A8
T7	Malware software	Stealing and modifying software data	External	Technical	A7,A8
T8	Data theft, modification	If the permission is not set, data will be viewed and modified	External	Technical	A9
T9	sql injection	The database writing language is not strict	External	Technical	A9
T10	natural disaster	Power failure caused by natural factors, machine damage	External	Physical	A10,A11
T11	DDOS	Large amounts of data visited the site, causing the site to stop working	External	Technical	A12
T12	The crawler	Malicious access to website data	External	Technical	A12
T13	Privilege separation	Employees gain too much access and steal customer information	Internal	Technical	A13
T14	Malicious Deletion of data	Angry or resigned employees, delete tables in the database	External	Technical	A13,A14

4.risk

In the following table, I listed the risk of the website server first, which is the most direct and the biggest loss. Customers know TMXBank and conduct transactions on the website, so it is critical to keep the website server unblocked. The second is the confidentiality of documents, emails, some cases such as the loss of the secret key, there is no management key will leak secrets. Data backup can save data from loss or database attack. Finally, there are physical site hazards as well as decision-making and budgetary hazards.



#	Risk
R1	Official website blocked
R2	File system, mail system stolen secrets
R3	Mobile app login security
R4	The firewall is damaged or invalid
R5	Data is lost during server upgrade
R6	Database data Loss(man-made)
R7	breach of PII
R8	Overbudgeting leads to loss of profits
R9	Server Power outages
R10	Workstation fires
R11	strategy mistake