Risk Assessment

* Define the Objectives and Constraints

“To achieve reasonable levels of security for reasonable cost”, for the case of individual bank account, that is to minimize the potential loss of funds and information within the budget of security investment.

* Identify the relevant Stakeholders, Assets, Values and categories of Harm
* Stakeholders

In the case of an individual, or a consumer, the primary stakeholder is the bank account owner -- myself. Others include my family, my employees (if I am a boss and pay salary to my employees), my business partners, my creditors or debt owners, the bank client manager who serves me and so on. Generally speaking, all people who keep a financial relationship with me.

* Assets

The assets we mainly take into consideration are data.

|  |
| --- |
| Relevant Data Assets   1. Funds contained in my bank accounts 2. Financial Data, e.g. records of transactions and assets, related financial product data, insurance and stocks details, tax records, debts 3. Payment Authenticators, e.g. PINs, credit-card CVV numbers and other details 4. Identity Authenticators, e.g. passwords, passport and driver’s license details 5. Personal Data of a sensitive nature: 6. Of myself, e.g. contact numbers, addresses, birthday and age 7. Of my family, e.g. Family Trust 8. Of others, e.g. Business Partner Contacts, contract details, company financial condition (if I am a boss) |

* Values

We mainly focus on the value attached by stakeholders to data.

|  |
| --- |
| Relevant Values Associated with Data   1. Accessibility: the data is always accessible to myself and to those under my permission. 2. Inaccessibility: the data is never accessible to those without my permission. 3. Quality 4. Accuracy: the amount of funds, every record of transactions, all financial details. 5. Precision: responds to its definition. 6. Completeness: covers all aspects needed and not misleading. 7. Timeliness 8. Currency: short time lag between occurrence and recording, especially the money arrival rate. 9. Temporal Applicability: always keeps the pace with changes in real-world. |

* Categories of Harm

Harm to values in data needs to be considered at two different levels.

|  |
| --- |
| Harm to Values Associated with Data   1. Accessibility 2. Data Loss 3. Data in volatile memory maybe be lost due to device and electric problems, e.g. payment failure and transfer failure. 4. Data in non-volatile memory is at risk of being over-written or mistakenly deleted in database. 5. Physical data storage-devices are subject to theft, destruction and malfunction. 6. Data Unavailability at a relevant time, caused by system shortfalls or work staff mistakes, leads to financial loss. 7. Inaccessibility: data in storage or transit is accessed or communicated to people without my permission or even without my awareness. 8. Quality: the data doesn’t satisfy all dimensions of data integrity, e.g. records mistakes, lack of essential account data. |

|  |
| --- |
| Harm to Stakeholder Values Arising from Harm to Values Associated with Data   1. Reduced Asset Value, e.g. loss of funds. 2. Degraded Operational Capacity, e.g. purchase or money transfer cannot be performed. 3. Degraded Service Quality, e.g. delay of payment leading to fines. 4. Cost, Time, Effort and Economic Loss Incurred during Recovery, e.g. cash flow interruption, loss of interests. 5. Damaged Reputation, e.g. influences the trust between employer and employees, business cooperation. 6. Negative Privacy Impact on Individuals, e.g. disclosure of personal information. 7. Non-Compliance with Obligations or Commitments, e.g. through loss of tax records. |

* Analyze Threats and Vulnerabilities

Here we’d like to identify distinct lists of vulnerabilities and threats.

|  |
| --- |
| Data Vulnerabilities   * Infrastructural Vulnerabilities   Dependence on the availability, reliability and integrity of:   1. Power Supply, subject to the threats of UPS failure, e.g. bank sever failure. 2. Networking Facilities, subject to the threats of outages and congestion, e.g. internet interruption. 3. Storage-Media, subject to the threats of disk crash, corruption, encryption, loss, online accessibility of live and backup data at the same time, etc. 4. Automated Process, subject to the threats of design and coding errors, malware, wrong versions of software, etc.  * Human Vulnerabilities   Dependence on the availability, reliability and integrity of individuals, subject to the threats of inadequate performance, training, loyalty and insufficient wariness and skepticism, e.g. business level and work attitude of bank staff, degree of caution of myself. |

|  |
| --- |
| Threats to Data   1. Environment Event, e.g. electrical event leading to sudden interruption, fire event and water event causing serious physical damages. 2. Attack 3. On Data Storage, e.g. theft and illegal access without my permission. 4. On Traffic, e.g. account being monitored. 5. On a Business Process, e.g. bank staff abuses privilege. 6. On a Computer-Based Process, e.g. malware against net bank account. 7. Accident 8. By Human, e.g. mistaken account number while transfer, bank staff operation mistakes. 9. Within Infrastructure, e.g. equipment failure, storage-device failure, bank network malfunction. |

* Identify existing Safeguards

Since the safety of bank accounts is of great importance to almost everyone, there are a great deal of safeguards in different levels.

Common patterns of human behaviors such as caution, customer habit while dealing with bank accounts, training of bank staff.

Physical site security methods such as the secure system of banks help as well.

Hardware and software designs in bank machines like ATMs and net banks, ensure the security in the level of codes, such as parity-checking, read-after-write, authentication of data required, access control, etc.

Logical security precautions are widely used, such as passwords, password protection questions and so on.

For net bank, network safeguards including channel encryption, firewalls and intrusion detection are provided by banks.

What’s more, legal measures, insurance and customer contracts are all kinds of safeguards.

* Identify and Prioritize the Residual Risks

Residual risks are those that are not satisfactorily addressed by existing safeguards. We choose the conventional approach to prioritization, that is to assign to each residual risk a severity rating and a probability rating, then sort them into descending order.

|  |  |  |
| --- | --- | --- |
| Risk | Severity Rating | Probability Rating |
| Malware attacks on net bank accounts | Extreme | Extreme |
| Attack by human, swindlers aiming at bank accounts | Extreme | High |
| Personal information disclosure | High | High |
| Operation mistakes by bank staff or account owner | Medium | Medium |
| Bank system or database crash | Extreme | Low |

Risk Management

* Identify alternative methods that will address the priority risk

As we defined in the previous section, we believe that malware attacks on net bank accounts are the priority risk for individual bank consumers since financial behaviors rely more and more on digital data through years.

There are different levels of safeguards and security strategies respond to this issue.

To ensure internal security, it may need both the effort from bank servers and consumer themselves. Access control by banks comes the first. Common safeguards towards access control include channel encryption, vulnerability inspection, threat detection and safeguard testing. As for customers, they may need to get fully prepare on backup and recovery, business continuity and disaster recovery. For instance, the most common way to do so is choose a reasonable anti-malware software and check the condition of accounts and devices periodically. Also, customers should try their best to avoid simple and common-used passwords and be careful of the environment every time the essential information of their accounts is needed.

To ensure the perimeter security, inspection and filtering are most useful methods. Most potential dangers come from external Internet. Thus, setting up firewalls and blocking out most potential threats automatically provide good help.

For external security, it covers content transmission security, authentication of sender, recipient and content, network-based intrusion detection and so on. Alternative choices include to implement SSL/TLS, VPNs and dig sigs.

* Evaluate the alternatives against the Objectives and Constraints

Since the issue we discuss is the safety of individual’s bank account, safety methods like access control may seem too costly regarding the effects. Methods to ensure external security will have to give priority to those for internal security and perimeter security.

* Adapt or refine the alternatives to achieve an acceptable design

In order to find a best balance between the degree of security and cost, we would choose such method to mitigate the risks from malwares: first, set up well-developed firewalls to filter most potential threats and update it periodically; second, choose a reasonable anti-malware and install it in all devices which will be used to take net bank operations; finally, make sure you’re fully equipped with good safety habits, e.g. set complex password and avoid unfamiliar environment.