Group Members ;Ijiehon, Ehis; Hussain, Areeb; Aboualnaga, Khaled

Assignment 3

Business model of BU Banks

Automotive companies use a financial services sector as a second mainstay with the intention of making profits. Mainly a combination of the sale of a valuable object, e.g. cars or trucks, and the offer of financial services is used. The bank offers customers financing models such as a loan to finance their car. Furthermore, the bank supports and finances the development and manufacturing of new cars and does not charge high interest rates like an external bank would. In summary, providing the benefits of a bank to customers as well as for the own company, an automotive company broadens the range of services so that they can earn money on a larger scale.

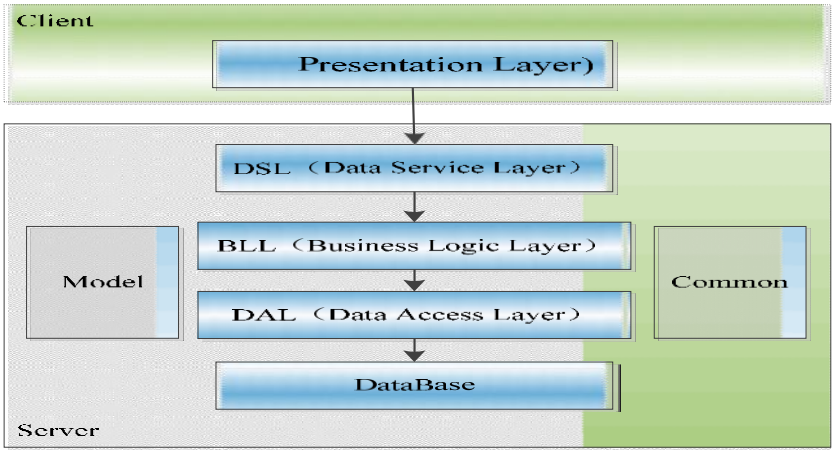
Importance of information technology for BU Banks

The obvious reason for the importance of cyber security in banking sector transactions is to protect customer assets. In this digital age, it is not only cyber fraud but hacks into servers to obtain a customer's personally identifiable information (PII). Hence, the reason why cyber security in banking is of utmost importance. As individuals and companies perform most transactions online, the risk of a data breach increases daily. Therefore, there's a greater emphasis to examine the importance of cyber security in banking sector processes.

Assets

Presentation layer
ATMs, Call centre & telephone/Email system, Online Banking
Data service Layer
Transaction Logs, Proprietary Software
Business logic Layer
Web servers, Master & Slave database servers, Network infrastructure, & online form-Software Licenses/Patents,
Data access Layer
-User Data, Employee/Employer Data, Financial Data, Backup System & off-site Backups

4-tier architecture for
Distributed IT systems



Taken from google images

CIA analysis for whole company (Cars, Bank, Trucks)

Banks:

- Servers for account transactions and the master database server require max priority for integrity/confidentiality over availability to ensure data can't be modified without authorization, accountability and financial data won't leak into public.
- Public web servers for new customers and the distributes storage & backup systems require highest availability and failover systems to ensure business continuity
- Internal online banking (app) require high confidentiality to ensure the security of private data and back-end servers for support of the online services and support require high integrity and some fail over
- Slave database servers provide higher availability while still maintaining confidentiality via authorization but easier and therefore lower priority on integrity through read-only mechanisms and checks with other servers in the network required to agree to modification

	Confidentiality	Integrity	Availability
Transaction servers for business customers:	10	10	0
Public webservers for new customers:	0	0	10
Online banking servers for private customers:	5	0	7
Administration servers for support/dev:	0	9	1
Backhand servers for information management (CMS):			
Master:	10	10	10
Slave:	8	3	5
Distributed storage and Backup servers:	5	5	10

Trucks:

- production services like web server and database back-end for it require high availability and fail-over to ensure business continuity while the latter requires also integrity because it contains only non-personal order information
- the manufacturing services require high availability to ensure business continuity in the manufacturing of trucks, the costumer database required for fulfilling the orders and distributing the products requires high confidentiality because it contains personal data, integrity priority is low because this information can be presented read-only
- the telemetry services for existing customers require high availability with fail-over to ensure 24/7 connectivity to guarantee no outage in service of the trucks

	Confidentiality	Integrity	Availability
Production:			
Webserver (Order Placement):	0	0	10
Order database:	0	4	10
Manufacturing:			
Information exchange server:	0	0	10
Customer database:	10	0	10
Service:			
Telemetry Services:	0	0	10

Cars:

- production services like web server and database back-end for it require high availability and fail-over to ensure business continuity while the latter requires also integrity because it contains only non-personal order information
- the manufacturing services require high availability to ensure business continuity in the manufacturing of trucks, the costumer database required for fulfilling the orders and distributing the products requires high confidentiality because it contains personal data, integrity priority is low because this information can be presented read-only
-Cloud service servers require availability and integrity because of safety of customer.

	Confidentiality	Integrity	Availability
Customer: Webserver and database (order Placement):	5	2	7
Production: Manufacturing and Automation:	0	6	10
Development: Computer aided design and simulations:	8	6	2

Overall ISMS policy

- Information security of our company is highly necessary to secure our business goals
- **ISMS** provide a secure processing of business to ensure improvement and continuity without interruption by malicious parties or from internal and external threats.
- Objective of our policy is to protect the company's information assets through safeguarding its confidentiality, integrity and availability
- The Head of the company or CISO must convene an Information Security Committee composed of senior management or assign the role to an existing senior management committee. This Committee is responsible for ensuring the Policy is applied.
- The infrastructure of the company and the trained employees should be adequately equipped for handling deviation and exception.

Segregation of the main computer centre into different compartments and IT architecture

The main components of the IT architecture are Clients, servers and network devices. **Client** computers provide an interface to allow a computer user to request services of the server and to display the results the server returns. The **Server** receives this request and processes it. The bridge between the whole Client -Server architecture is **Network Devices** which connects them together, some examples are (Hub, Switch, Bridge, Gateway, Modem, Repeater, and Access point etc.

Companies segregate a network and apply appropriate controls by breaking the network into multiple attack surfaces that prevents threat agents from reaching their critical network resources .
Publicly accessible servers get physically separated from internal servers with high confidential data and only connect through interfaces to the internal servers which require authentication and access control. These internal Servers are in their own DMZ network and isolated from the rest of the company.
High Availability servers like e-Mail, Web and Online-Banking (front-end) are distributed across the world and internal across the manufacturing departments to provide fail-over and 24/7 Service. Configuration and Slave Database servers offering less confidential but still critical data get are local to the public services to minimize latency.

Top security threats

Vulnerabilities in your company's infrastructure can compromise both your current financial situation and endanger its future. Companies everywhere are looking into potential solutions to their cybersecurity issues. Below we discuss some threats that an automotive company faces.

1) Threat Scenario: Data Breach

Data Breach is the loss of private/secure data by a company. It has a big importance for both customer and business side. The loss can occur mainly because of human beings. Often intentional by a hacker outside the company, but also unintentional by the staff or external staff.
Targeted assets: Customer data, employees

Security controls referring to ISO 27002:
A8.3.2 - Disposal of media

Control: Secure disposal of no longer needed media

- Media containing confidential information should be stored and disposed safely, for example shredded or incinerated.
- Procedures to identify data, which is important to disposing securely are necessary, but it can be easier to collect all media items and dispose them then.
- Be careful with organizations which offer collection and disposal services of media, ideally do it yourself.

A12.3.1 - Information backup

Control: Regular backup of information, software and system images

- Accurate and complete records of the backup copies and documented restoration procedures should be produced.
- The extent and frequency of the backups should conform with the security requirements and the business requirements.
- The backups should be stored in a remote location, with a sufficient distance to the main location.
- In special situations where confidentiality is important, the backups should be protected additionally, by encryption.

A13.2.1 - Information transfer policies and procedures

Control: Protecting the transfer of any information by formal transfer policies, procedures and controls

- Procedures which prevent transferred information from getting intercepted, copied, modified, miss-routed or destroyed.
- Procedures for the detection and protection against malware.
- Use of cryptographic techniques to protect the confidentiality, integrity, and authenticity of information.
- Advising personnel to take appropriate precautions not to reveal confidential. information.
- Not leaving messages with confidential information on answering machines.

2) Threat Scenario: Exploitable Software Vulnerabilities

A vulnerability with one or more known instances of working and fully implemented attacks is classified as an exploitable vulnerability — a vulnerability for which an exploit exists. A resource may have one or more vulnerabilities that can be exploited by a malicious person in a threat action. The result can potentially compromise the confidentiality, integrity or availability of resources belonging to an organization and/or other parties involved. Example scenario:

An attacker finds an exploit in the public accessible servers and services. Through exploit of the software the attacker may installs and execute “ransomware” type **malware** on the **IT infrastructure**, either infecting a network of computers (PC/Servers) or individual PCs holding production data. The ransomware encrypts this data in-place which, meaning that the original data is deleted, overwritten or otherwise made inaccessible. For the attack to success and ransom the data, the encrypted data has to be encrypted using a secret key, this **key** is unique, only held in memory and encrypted using the attackers accessible public key (usually hard-coded in ransomware). After the ransomware software was able to finish encrypting all data and making the original data inaccessible without interrupting (e.g. reboot) the software usually presents a document explaining the situation, including the encrypted secret key and a request to pay to get the secret key de-crypted and therefore be able to decrypt the data and recover the original data.

Targeted assets: Customers, Money

Security Controls referring to ISO 27001:
A12.2.1 - Controls against malware

Control: Protect information and information management facilities from malware and raise appropriate user awareness

- Implement detection, prevention, and recovery tools against malware by prohibiting unauthorized software via whitelisting.
- Installation of malware detection systems which scans all types of incoming files e.g. via network download or USB media, for malware, and which scans mail attachments when they enter the mail server and scan webpages for malware.
- Define procedures to deal with malware infection like reporting the incidents and executing an already implemented business continuity plan.

A12.6.1 - Management of technical vulnerabilities

Control: Gather and evaluate information about technical vulnerabilities and take appropriate measures to address them

- Prevent exploitation of technical vulnerabilities by defining management and monitoring roles for them.
- Patching and assessment of necessity by evaluating if patch fixes present vulnerability appropriately and if new risks arise by patching.
- Patch testing before implementation in a safe environment and increase of monitoring and logging to track suspicious behaviour and detect it in a timely manner
- Communication with incident management about vulnerabilities and risks by setting up emergency plans like backup servers and software.

A13.1.1 - Network Controls

Control: Ensure security of information in networks and the protection of connected services from unauthorized access.

- Separation from operational responsibility for networks by introducing a network operation centre, which is a specific department for network management, monitoring and controlling.
- Logging and monitoring of traffic and using intrusion detection and network security monitoring software, like security onion, forensics analysis of collected data to track suspicious behaviour.

• Authentication of network systems by requiring login for a network action such as a file transfer and restricting access of systems connected to the internet.

3) Attack Vector: Social Engineering

Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. Although it is like a typical confidence trick, the concept is applied to the trick of gathering login credentials, bank information or computer access, and it's commonly one of the many steps of a bigger scheme.

Initial Targeted Assets: Customers, employees and third parties' employees.
Goal Targeted Assets: Money, holdings, and securities.

Security Controls referring to ISO 27001:
A.7.2.2 – Information security awareness, education, and training.

Control: All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

- Conduct security training for new employees adapted to their role and access.
- Conduct security training for employees when they change area and level.
- Reinforce security with follow-up trainings on a regular basis.

A.7.2.3 – Disciplinary Process

Control: There shall be a formal and communicated disciplinary process in place to act against employees who have committed an information security breach.

- Establish different levels of disciplinary process based on nature and gravity of a breach, while ensuring correct and fair treatment of employees.
- Establish a reward system for employees that successfully follow security procedures.
- Include clauses in personal contracts for their understanding and acceptance of the disciplinary process.

A.9.2.2 – User Access Provisioning

Control: A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services

- Include clauses in personal and services contracts, regarding the acceptance of responsibilities for unauthorized use of access.
- Adapt and update access, so it is limited to the necessary business requirements according to the user role.
- Maintenance of a central record with access and activity information, to facilitate tracking the origin of any breach.

4) Threat Scenario: Damage or Sabotage of data storage facilities.

A threat scenario like this has potentially so greater consequences for the company that the affects could be felt in the longer term as well. It has the potential to completely shut down the working capacity of the company and halt all manufacturing and businesses. However natural catastrophes that could cause such a scenario for e.g. earthquake, fire, flooding, explosion at that magnitude are a rarity but still it is necessary to prepare for the worst case especially concerning sabotage by humans.
In the case of one of these events happening buildings and the servers and data processing facilities located in them could be destroyed. It is difficult to estimate the damage caused by one of these incidents. Depending on the nature of the event, there is the possibility of a temporary or complete failure of all products and services of the entire company.

It is especially important to prepare for these events, as in some cases they are not easy to prevent. Although in some cases it is possible to prevent incidents for example unauthorized humans entering and damaging the facilities.
Targeted Assets: Company's data storage facilities/ buildings

Security Controls referring to ISO 27001:

A. 11.1.4 – Protecting against external and environmental threats

Control: It is the goal to prevent unauthorized physical access and damage and interference to the organization's information and information processing facilities.

- It is advised to search specialist advice to avoid damage from fire, flood, earthquake, explosion civil unrest and other forms of natural or man-made disaster.
- We could also invite an expert in fire protection and following the expert's advice and equipping rooms in an appropriate way

A. 11.1.3 – Securing offices, rooms and facilities

Control: Network Segregation should be given utmost priority.

• It is advised to design facilities the way for them to not be accessible from outside to prevent unauthorized people from having access to the facilities

• servers / processing facilities should be separated or surrounded by other buildings so possible intruders have no easy access to them.

• Physical security for offices, rooms and facilities should be designed and applied.

5) Threat Scenario: Staff leaking confidential information.

Company employees who might have access to sensitive information may be a potential threat to the company as well. They could willingly disclose or give access of this information to third parties. However, this could happen unintentionally as well, if they let their computer screens unattended without logging off. Even things like leaving passwords on written piece of paper can have fatal consequences

Targeted Assets: Company/ production data/ intellectual property theft

Security Controls referring to ISO 27001:

A. 11.2.8 – Unattended user equipment

Control: The employee is obligated to terminate all active sessions when the workspace cannot be attended at the time.

• It is necessary to lock every device that is used for work related tasks with e.g. a password.

A. 11.2.9 – Clear desk and clear screen policy

Control: A clear desk policy for papers and removeable storage media and a clear screen policy should be adopted.

• all sensitive or critical business information e.g. on paper or removeable storage devices should always be locked away when not needed

• Only authorized personnel should be allowed to use photocopiers

•all media that contains classified data for the organization should immediately be removed from those reproduction technologies.