Project, INSE 6680

PHYSICAL SECURITY IN FINANCIAL INSTITUTIONS

by
Pavithran Koteeswaran – 40196178
PriyaDharshan Muthu - 40196410

Concordia Institute for Information Systems Engineering (CIISE)

Concordia University

Winter. 2022

TABLE OF CONTENTS

CONTENTS

Chapter 1

Introduction

Financial institutions/banks are the safest places to store cash, documents, valuable items, etc. Nevertheless, bank system failure, Robbery, and Cyber-attacks are inevitable. It is a key role to implement optimal security policies for both online and traditional banking systems. These security policies include both Physical and Cyber Systems.

Chapter 2

Physical Security Systems of Financial Institution

The overall objective is to provide physical security among financial facilities within the financial services industry.

This study focuses on identifying the top risks/threats, the current physical security technologies used to manage/minimize risks, and their integration while also examining the decision-making and budgeting processes when choosing physical security technologies

The financial services sector tries to manage and minimize risks and challenges, among which the most important are: unauthorized data access, cyber-attacks, and unauthorized entry. To manage these challenges, financial services adopt physical security systems and technologies such as CCTV surveillance, Access control systems, Damage and recovery control, and best Infrastructure practice.

Chapter 3

Infrastructure

Objectives Covered in this Chapter include:

3.1 Building Perimeter

For an organization to be less vulnerable to security threats, resilient building infrastructure is essential.

Security is influenced by factors such as location, environment, natural physical barriers, and infrastructure protection.

An established physical perimeter line separating secure and nonsecure areas around a building is the last line of defense against threats approaching within a building's reach.

For high-risk facilities, organizations may consider the use of perimeter protection by utilizing fencing or wall barriers.

Key considerations such as construct, deployment, and height are important when evaluating the use of security fences or wall barriers.

To provide extra security or make breaching the perimeter protection measure more difficult, lighting, CCTV surveillance or intrusion detection systems may be deployed.

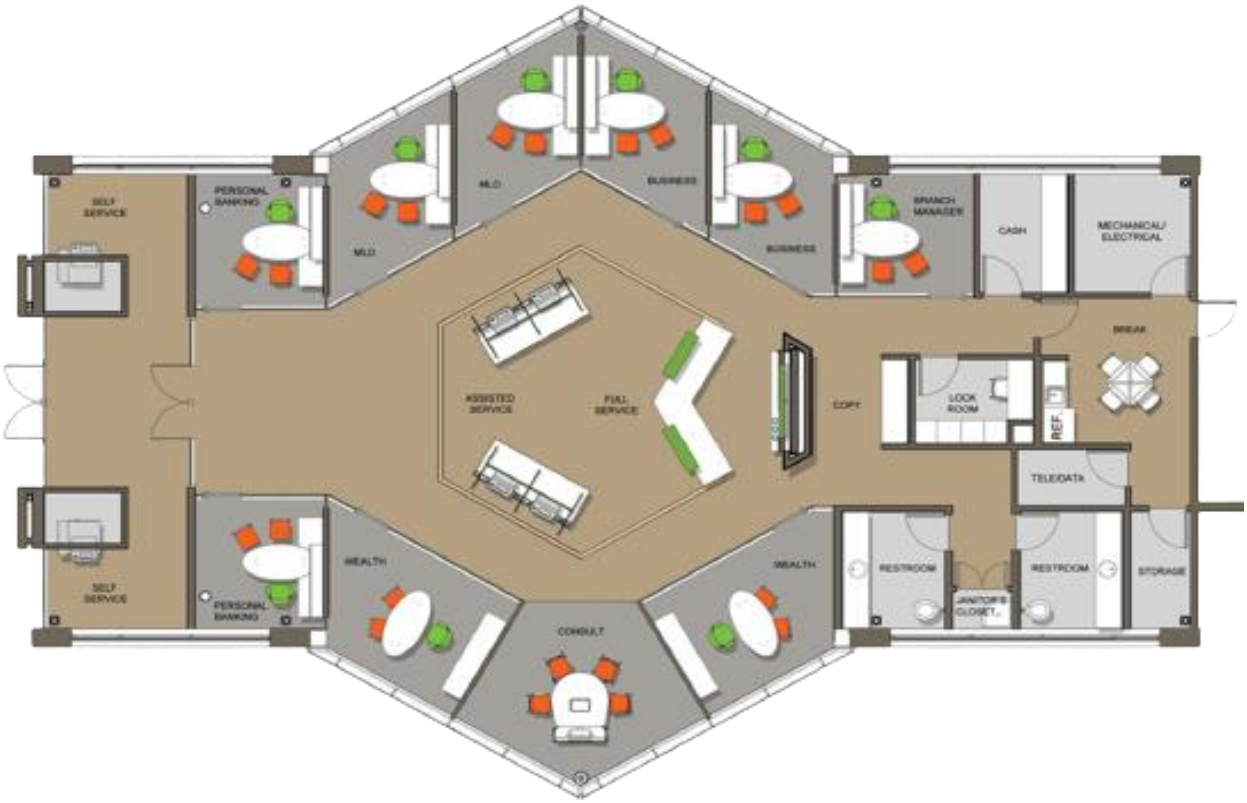

Figure 3.1.a

3.2 Entry Points

The first line of defense at a bank is the front door, which is designed to allow people to enter and leave while providing the first layer of defense against attacks.

Past the entrance, there is often a security guard, which serves as a second line of defense. This "security guard," seeks to identify unusual behaviors or other indicators that signal that trouble has entered the bank, such as somebody wearing a ski mask or perhaps carrying a concealed weapon.

Exterior doors and windows should be of sturdy and fixed construction, with secure locking devices. External glass facades, doors, or windows vulnerable to damage may require additional protection such as the use of tempered glass or shatter-resistant film.

CCTV surveillance and intrusion detection systems may be deployed as complementary security measures at entry points.

Entrances should be prioritized and kept to a minimum.

The areas with restricted access such as external doors and windows should be closed to the public.

Door access control ensures that movement is controlled by determining which individuals have access to which areas.

Based on the following considerations, a plan to prevent unauthorized entry or delay intrusion can be developed:

- In buildings, offices, branches, and critical facilities, what entry points exist?
- Is entry point control constructed and made of strong materials?

- Can turnstiles or gates be installed to mitigate these vulnerabilities?

3.2.1 Types of entry points (Security Door)

SLIDING DOOR

figure 3.2.1.a

STEEL DOOR

figure 3.2.1.b

REVOLVING DOOR

figure 3.2.1.c

MAN TRAP DOOR

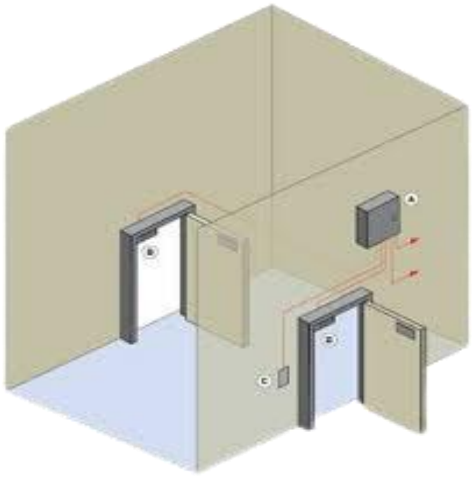

figure 3.2.1.d

GATES

figure 3.2.1.e

BLAST/BALLISTIC WITHSTAND DOOR

figure 3.2.1.f

3.3 Internal Access Points

Depending on the sensitivity of the area, all internal access points should be designed with a proper level of security.

In addition to outside entry points, internal entry points should be equipped with lighting, surveillance cameras, and hardware controls connected to an IP network that can be accessed anytime anywhere.

Furthermore, access points to restricted or critical areas should be designed with complementary controls such as MFA, intrusion detection systems, and audible alarm systems.

Maintaining bank servers and network access points inside the building is also an important aspect of preventing cyberattacks, such as wireless network attacks and DDoS attacks.

Preventing any attacks against these areas should be our priority.

3.4 Special Facilities

3.4.1 ATM (AUTOMATED TELLER MACHINE)

Among the ways in which criminals compromise the physical security of an ATM are card skimmers, crowbar smash-and-grab attempts, and other brute-force attempts to open or remove the ATM from the site.

A cyberattack on an ATM targets computer systems, applications, networks, and data.

These are some of the ways where we can protect ATMs from Physical attacks:

- To establish a perimeter security plan before installing a device.
- To ensure the cameras and other security devices regularly to ensure they are in good working order
- To constantly monitor with a consistent, standardized control approach and protocols (Card Reader Check, For suspicious activities, etc..)

3.4.2 VAULT ROOM

A vault or safe room is designed for the safekeeping of valuables including cash and negotiables

Safes and vaults can be fire-resistant (both document and data), burglary-resistant, or a combination of both.

CCTV surveillance and intrusion detection systems must be deployed to provide additional security or increase the difficulty of breaching the vault perimeter.

Vaults and safes must be provided with biometrics or access tokens to classified people for authentication to provide additional security.

To prevent robbery, vaults and safes must be built and placed deep inside the infrastructure, which provides more protection and increases the time during invasions.

Vaults are classified by Underwriters Laboratories (UL) based on the length of time their doors and walls can defend against a burglarious attack. The four classifications are as follows:

- *Class M* – 15 minute
- *Class 1* – 30 minutes
- *Class 2* – 60 minutes
- *Class 3* – 120 minutes

figure 3.4.2.a

figure 3.4.2.b

3.4.3 MAILROOMS

A mailroom receives stores and distributes the building's mail streams, including mail, parcels, and deliveries.

The mailroom is a high-risk area, so it needs adequate protection, such as CCTV surveillance and access control systems. It should also be restricted to authorized personnel only.

The incoming mails and parcels must be screen-tested to prevent any illegal items or sometimes to prevent them from booming.

For safety reasons, mailrooms should be placed in a separate facility within the building away from critical areas.

Identifying and responding to threats in the mailroom should be part of proactive security training.

Chapter 4

SECURITY SYSTEMS AND ACCESS CONTROL SYSTEM

Objectives Covered in this Chapter include:

4.1 CCTV Surveillance System
4.2 Alarm System
4.3 Physical Access Tokens
4.4 Biometrics
4.5 MFA

4.1 CCTV Surveillance System

When your bank is set up with a top-notch surveillance system, it acts as a deterrent for criminals who might otherwise try to hold your bank up. If they still proceed to rob you, at least you will have their images on the video to assist authorities in apprehending and prosecuting the bank robbers.

Advantages of CCTV Surveillance

- Deters check fraud
- Prevents robberies
- Monitors ATM withdrawals
- Intelligent cameras
- Digital storage Data recognition
- Greater customer confidence
- IP Cameras

4.2 Alarm Systems

Alarms serve to alert operators to abnormal conditions

Physical security can involve numerous sensors, intrusion alarms, motion detectors, switches that alert to doors being opened, video and audio surveillance, and more

But an alarm is the easiest method of alerting personnel to the condition.

Though alarms are the easiest method for implementation and maintenance, Alarms are not simple, if a company has too many alarm conditions, especially false alarms, then the operators will not react to the conditions as desired.

Tuning alarms so that they provide useful, accurate, and actionable information is important if you want them to be effective

4.3 Physical Access Tokens

A security token is a physical or digital device that provides two-factor authentication (2FA) for a user to prove their identity in a login process. It is typically used as a form of identification for physical access or as a method of computer system access.

The most common types of physical tokens are smart cards and USB tokens, which require a smart card reader and a USB port respectively.

TYPES OF SECURITY TOKENS:

- Smart cards
- Contactless tokens
- Bluetooth tokens
- NFC tokens
- Single sign-on software tokens
- Programmable tokens

4.4 Biometrics

Biometrics fits exactly the "What I am" group of identification techniques because it measures an individual's unique physical or behavioral characteristics.

- Fingerprint recognition,
- Finger or palm veins,
- Facial recognition (with liveness detection),
- Voice recognition,
- Iris scan.

Enrollment: performed once per device. This creates reference data to be securely stored in the device and then used for comparison when a verification request is completed. The user can do the enrollment process online or with a bank employee's assistance at the branch.

Verification: performed each time the users want to identify themselves. This step ends a biometric capture that's then compared with the reference data.

Biometric Modality	Accuracy	Cost	Size of template	Long term stability
Facial recognition	Medium/High	Low	Small*	Medium/High
Iris scan	High	High	Small	Medium
Fingerprint	**High**	**Low**	**Small**	**Medium**
Finger vein	High	Medium	Medium	High
Voice recognition	Low	Medium	Small	Low

* Between 1-2 KB, depending on algo type (Standard vs. LITE)

4.5 Multi-Factor Authentication

MFA Device Security:

Electronic fingerprint: MFA Device Security examines the customer's computer and registers it based on several characteristics to create a one-of-a-kind electronic fingerprint that it verifies each time a customer logs in.

Supplemental authentication: For customers with more than one PC, supplemental authentication confirms the user's identity. This authentication may include answering questions, or entering a one-time password received via email

MFA Security Tokens:

Quick activation: Delivered in an unregistered state, tokens are activated by customers during their Internet banking session. It takes just a few seconds to gather a token's serial number and define a PIN. A security question and email address are also gathered to assist in reporting a lost or damaged token

Customizable tokens: Available for licensing in a variety of styles, tokens can be customized to fit your financial institution's corporate branding

Chapter 5

TRUSTED SUPPLY CHAIN

Financial institutions need to work with vendors who manufacture all aspects of their cameras or security system products and who control their distribution.

End-to-end, in-house manufacturing is the best way to ensure that parts and chipsets are built following best practices.

When a vendor controls all aspects of manufacturing, it also provides customers with peace of mind because they know that any upgrades or changes are coming directly from the vendor rather than a third-party manufacturer.

A vendor with strong cyber hygiene can help financial institutions install the advanced solutions they require to mitigate the risks of cyber threats.

Chapter 6

CONCLUSION

Good security starts with good physical security control. Knowing who is in the building and that they have the correct authorization to be where they are is vital to keeping your people and your property safe.

An access control system is a tool that makes the process significantly easier and more streamlined than the days of having to issue physical keys.

Plans should be developed and implemented to ensure that corrective actions are taken to address the enhancements of security measures.

Chapter 7

REFERENCES

https://www.nimbleplanet.com/industries/bank-security-camera-systems/

https://www.techtarget.com/searchsecurity/definition/security-token/

https://abs.org.sg/docs/library/abs-scps-guidelines.pdf

https://bankingjournal.aba.com/2021/09/four-key-physical-security-measures-for-financial-institutions-to-protect-themselves-from-cybercrime/

https://www.greetly.com/blog/physical-security-access-control-systems/

https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/cards/biometrics-in-banking

https://www.fiserv.com/en/who-we-serve/financial-institutions/banks/bank-platforms/multi-platform-solutions-for-banks/