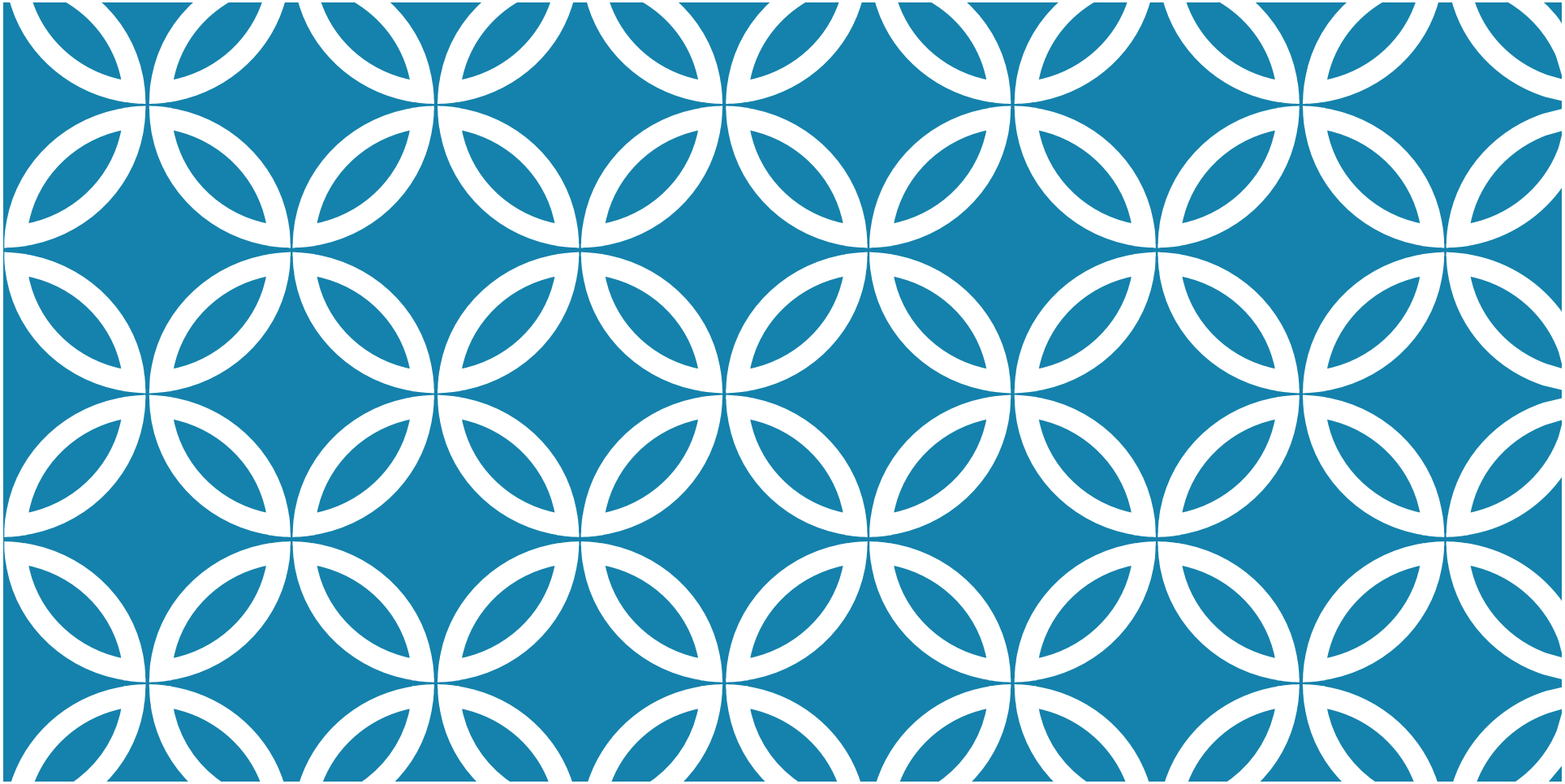


WIE3003: INFORMATION SYSTEMS SECURITY AND CONTROL

Physical Security VS Logical Security

LEARNING OBJECTIVE

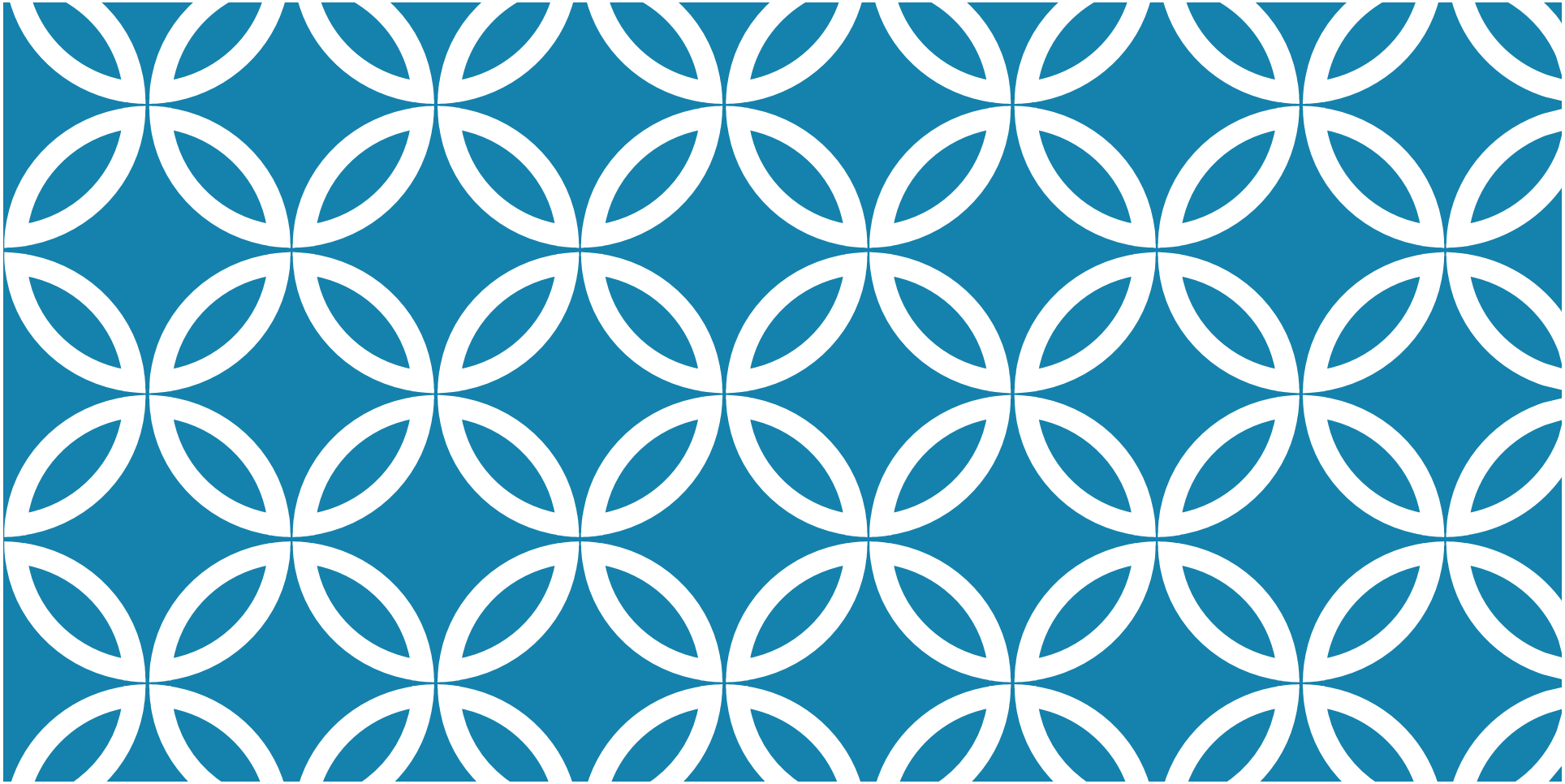
To discuss the physical security vs the logical security

To understand the difference between preventive and deterrent measures

SECURITY LAYERS

https://www.youtube.com/watch?v=kd33UVZhnAA&t=19s

https://www.youtube.com/watch?v=XZmGGAbHqa0



PHYSICAL SECURITY

PREVENTIVE CONTROLS

1) Various types of physical locks, including conventional key locks, electronic access badge locks, cipher locks, combination locks, and biometric locks
2) Security guards
3) Video surveillance cameras
4) General emergency and detection procedures
5) Heating, ventilation, and cooling (HVAC) systems
6) Insurance coverage over hardware and the costs to re-create data
7) Procedures to perform periodic backups of system software, application programs, and data as well as storage and rotation of the backup media to a secure off-site location
8) Emergency power and uninterruptible power supply (UPS) systems
9) Current and tested business resumption program (BRP), including key aspects of an information systems BRP
10) Adequately trained backup system security administrators

PHYSICAL LOCKS

1. *Conventional keys* can still be one of the most effective means of controlling access to restricted rooms. Only to highly trusted employee.

2. *Electronic access badge.* First advantage: eliminate the need to have to issue conventional keys to all employees, rather provide them with the access they need. Whenever someone terminates, transfers, or loses his or her badge, it is simply deactivated on the electronic access badge system, thereby preventing any further access to previously authorized doors. Second advantage: electronic badge access can be restricted to certain times of the day or night.

3. A *cipher lock* is simply a lock that is opened by entering a secret set of numbers and/or characters on a keypad next to the door.

4. A *combination lock* requires that a secret set of combination numbers be spun on a dial in the appropriate sequence. Usually used to secure passwords, keys, and other information necessary in the event the primary system security administrator or control person is not available and changes need to be performed.

5. A *biometric lock* is one that authenticates a person by recognizing one or more unique physical features of the accessing individual. Such features include fingerprints, handprints, iris images, retinal images, facial images, voice recognition, or some other unique biological feature

SECURITY GUARDS

Security guards are an important component of an organization's overall physical security program.

Although the guards are not police, they are a deterrent to theft, danger in the workplace, and other illegal and unauthorized activity.

They also assist in reducing the incidence of piggybacking into data centers and in the monitoring of controls such as video cameras.

VIDEO SURVEILLANCE CAMERAS

Video surveillance cameras are an additional control that can act as an effective deterrent to unauthorized activities and provide critical evidence in criminal prosecution and employee misconduct.

Video surveillance cameras are usually positioned in strategic locations that afford full views of the doors and/or equipment they are designed to protect. The video system should be designed so that the day, date, and time appear on the recording.

These systems are designed so that the views appearing in the monitors rotate among the various video cameras periodically (e.g., every 30 seconds).

Security guard procedures should specify that they are to observe the activity in the monitors on a regular basis.

GENERAL EMERGENCY AND DETECTION CONTROLS

Alarms can be triggered by smoke, fire, or a number of other specific actions (e.g., forcibly opening a restricted door).

Alarms should be installed at strategic locations throughout a facility for both safety and security reasons.

Heat-activated overhead sprinkler systems are required in most facilities. They may or may not be located above computer equipment, depending on the local fire code and the wishes of management

Fire prevention systems that released pressurized halon gas in the event of a fire as it rapidly removes oxygen from the air, thus suppressing a fire.

Fire extinguishers are a simple but necessary component of the overall fire prevention control environment. They should be strategically located around the facility, especially in areas where the risk of fire is greatest.

A master key to all the doors in a facility is commonly located in a locking key box on the outside of a facility. The key box should be accessible only by the fire department.

Building blueprints should be on file with the local fire department and/or located in a restricted area that is accessible by the fire department

HEATING, VENTILATION, AND COOLING SYSTEMS

Computers survive best in a cool, dry, dust-free environment. Many computers do not require special HVAC equipment. Example, laptop, desktop computers function very well in a typical office or household room

Large mainframe computers generate significant amounts of heat, thus requiring special air-conditioning systems to maintain temperatures within manufacturer-specified ranges. Many mainframes also require special dust removal equipment because of the significant amount of air turbulence they create.

The comfort requirements of the people operating the equipment is a must. Computer rooms should not be so cold

Faulty or poorly maintained ventilation systems can lead to poor health of the staff. Failure to perform routine maintenance of ventilation systems is one of the most commonly overlooked procedures in many companies.

The role of an information systems auditor should be to ensure that the HVAC systems receive maintenance on a regular basis as required by the manufacturers.

INSURANCE COVERAGE

Insurance should be maintained to cover computer hardware and software at replacement cost and the costs to re-create lost data.

Some policies may even cover lost revenues that are directly attributable to computer hardware or software failures.

However, coverage for lost revenues may be costly and can be difficult to prove.

PERIODIC BACKUPS

Procedures should be in place to perform periodic (daily, weekly, monthly) backups of system software, application programs, and data as well as storage and rotation of the backup media (e.g., magnetic tapes, disks, compact disks [CDs]) to a secure off-site location.

Daily backups are usually necessary only for data since the application programs and system software do not change significantly. Full backups of the entire system, including system software, application programs, and data should be performed weekly or monthly, depending on the number and types of changes that have been made.

Full system backups should also be performed on completion of a major upgrade or significant changes to the operational and security parameters of a system.

Logs should be maintained to document that backups have been performed and that the backup media have been transported to the off-site location.

EMERGENCY POWER AND UNINTERRUPTIBLE POWER SUPPLY SYSTEMS (UPS)

An emergency power system consists of a generator and the necessary hardware to provide limited electrical power to critical operational areas within a facility. In the event of a power loss, the emergency power system should activate automatically.

A UPS system consists of an arrangement of batteries and supporting hardware components that are configured to provide smooth, continuous power to computer equipment.

The UPS system acts as a buffer between the outside power source and the computer equipment, so that power surges and spikes are minimized.

Also, in the event of primary power loss, a UPS system continues to supply electricity to the computer equipment until the emergency power system can fully activate.

BUSINESS RESUMPTION PROGRAMS

Business resumption program (BRP) also referred to as disaster recovery program (DRP).

The BRP should be as brief, concise, and easy to read as possible, while still retaining the key procedures necessary to ensure that all steps are carried out in a timely and appropriate manner.

BUSINESS RESUMPTION PROGRAMS

BRP must include:

1. **List of key contact personnel** throughout the organization, including contact phone numbers (home, work, cell phone, pager) and home addresses.

2. **Primary and secondary headquarters sites** where key management are to convene in the event that a disaster has rendered the main headquarters location inoperable.

3. **Identify and rank operational areas in terms of criticality and risk.** The high risk processes should be the first ones to be made functional in the event of a disaster. Data processing areas are usually at or near the top of the list of critical operational areas since so many other areas rely on data processing resources. Key aspects of a data processing BRP are discussed later in this section.

4. **Brief description of events that should trigger the BRP.** This section should include initial BRP procedures as well as procedures for escalating the BRP, depending on the severity of the situation.

5. **Concise descriptions of the actions that will take place in each of the operational areas.** These narrative descriptions may also include drawings and schematics of the facility.

6. **The potential psychological impact of the disaster on the ability of employees to perform their duties.**

KEY ASPECTS OF AN INFORMATION SYSTEMS BUSINESS RESUMPTION PROGRAM

Full-blown information processing disasters, an organization's BRP should provide for alternate information processing sites include: hot sites, cold sites, vendor sites, and reciprocal sites. (four alternative information processing site)

The type of site selected depends on the type of computing system platform (i.e., computer hardware and operating system), available financial resources, and desired time to full information processing capability at the alternative site.

FOUR ALTERNATIVE INFORMATION PROCESSING SITE FOR BRP

1. A ***hot site*** is an information processing facility that is fully equipped and configured with lights, electricity, air-conditioning equipment, computer equipment, and supplies such that it can be fully operational in less than 24 hours. The primary advantage of a hot site is its fast start-up time.

2. A ***cold site*** is a facility that is equipped only with the basic infrastructure necessary to operate the primary information processing system. The infrastructure includes lights, electrical wiring, air conditioning, and supplies but does not include the computer equipment. A cold-site plan provides for the organization to receive the necessary computer equipment from a vendor or alternative supplier within a predetermined period.

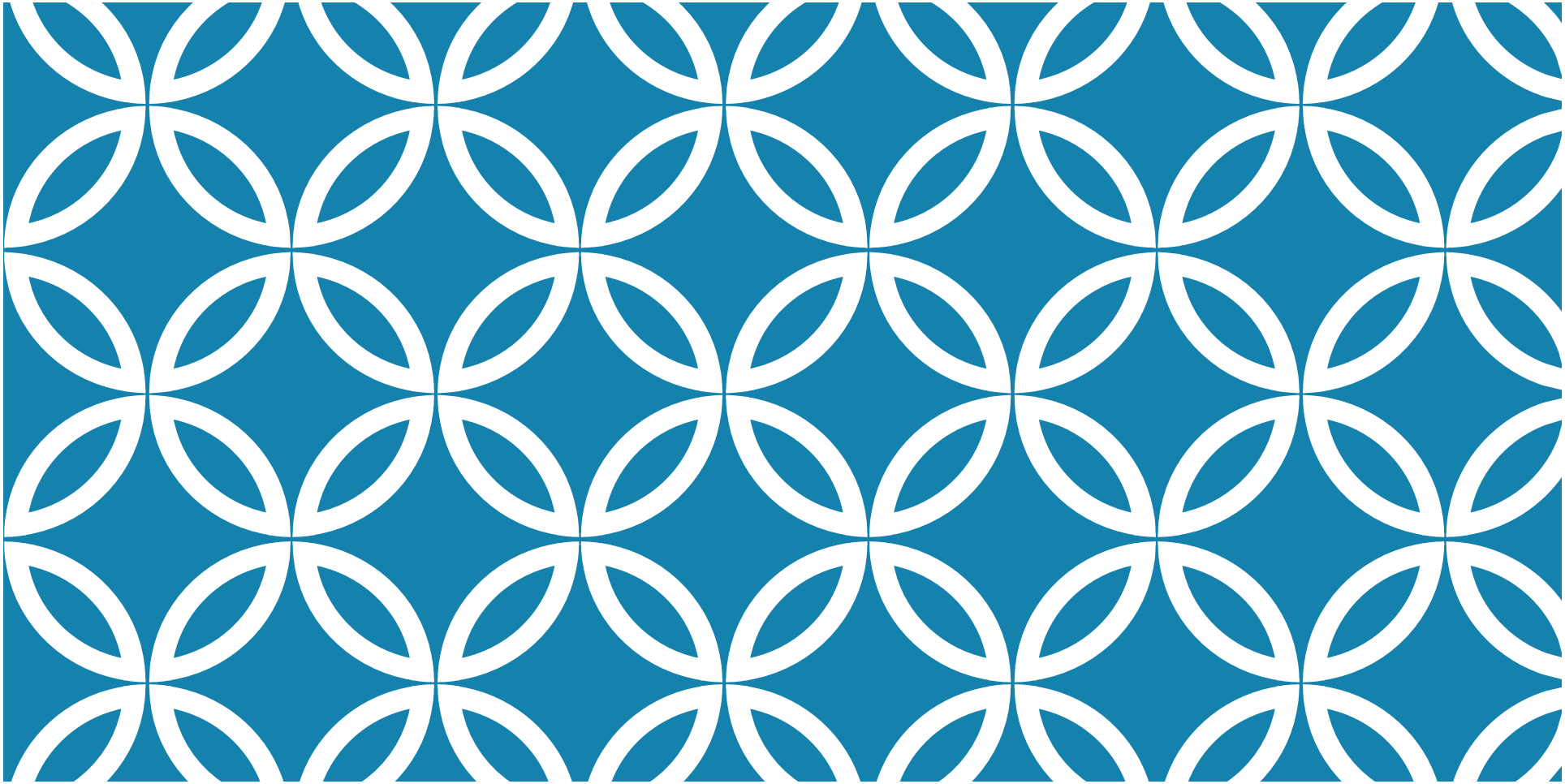
3. A ***vendor site*** is an information processing facility that is provided by a vendor that specializes in providing such facilities. Advantages include fast return to operations and elimination of the need to acquire and maintain a facility and related equipment. Disadvantages include a relatively high cost that the vendor may charge and the potential risk that the vendor's site is not maintained at full compatibility with the client organization's information processing system.

4. A ***reciprocal site*** is an information processing facility located within another organization. Two organizations form an agreement in which each agrees to allow the other to utilize its IS resources if one or the other experiences a business interruption.

BACKUP SYSTEM SECURITY ADMINISTRATOR

Granting complete control over a computer system to one individual is one of the most common control weaknesses in the real world.

Management of many organizations fail to recognize the need and urgency to designate and adequately train a backup system security administrator.



LOGICAL SECURITY

LOGICAL CONTROL

Logical controls reside in operating system, a database management system (DBMS), or an application program.

The degree of risk will have an impact on the types of logical security controls that need to be designed into the system as well as the number of controls and their relative strength.

LOGICAL CONTROL

One of the most difficult risks to control is the performance of unauthorized activities by a system security administrator.

By definition, a system security administrator needs to be able to add, delete, and change users and their access capabilities, monitor and regulate system activities, control system security parameters, review system security and operational logs, and perform various other unrestricted tasks.

To accomplish these tasks, a system security administrator requires virtually unrestricted access within the system.

DETERRENT CONTROLS: SYSTEM ACCESS

Two techniques can be designed into a system to control system security administrator activities:

1. Program the system to require a second system security administrator to confirm any additions, changes, and deletions of user IDs and their access capabilities and to make changes to system operating and security parameters.

Program the system to log all potential system security related events and implement procedures whereby the log is reviewed regularly for unusual or unauthorized activity. The system should also be programmed so that a system security administrator cannot delete or change the log file

DETERRENT CONTROLS: USER IDS AND PASSWORDS

The system should be programmed to recognize a *system user ID* and *maiden password*.

Password characters should not appear on the terminal screen as they are entered by the system security administrator.

This control is called *password masking*. Password masking makes it difficult for a passer-by or observer to steal another user's password and then perform unauthorized activities

PASSWORD PARAMETERS

Five common customizable system-wide security parameters include:

1. *Minimum password length.* The system should reject any user attempts to enter passwords with fewer characters than the parameter setting.
2. *Password expiration period.* When the password expiration period has elapsed, the system should prompt each user to enter the old password as well as a new password for change
3. *Number of consecutive unsuccessful sign-on attempts allowed before suspending a user ID*. If the number of unsuccessful consecutive sign-on attempts has been reached, the system should suspend the user ID.
4. *Time of day and day of week that users can sign on.* The system should reject any user attempts to access the system during times of the day outside the parameter settings.
5. *Period of inactivity allowed before a user is automatically signed off.* When a user ID has been inactive for the period specified in the parameters, the system should automatically save and close any files.

AUTHENTICATION FACTORS

An authentication factor is a category of credentials used to authenticate or verify a user's identity. Authentication factors can include passwords, security tokens (like keys or smart cards), and biometric verification such as fingerprint scans.

There are three main authentication factors:

1. **Something you know (aka knowledge factors):** This is the most common authentication factor. It verifies identity by confirming users through confidential information they have, such as a login and password.

2. **Something you have (aka possession factors):** Users verify their identity with a unique object such as an access card or key fob. This authentication removes the risk of forgetting passwords; however, it means the user must have the object with them whenever they need to access a system, and they run the risk of losing it by accident or theft.

3. **Something you are (aka inherence factors):** An inherence factor verifies identity through inherent biometric characteristics of the user—like a fingerprint, voice, or iris pattern. The advantage of biometric authentication is that they're harder to lose or replicate. But they can be expensive and less accurate than traditional authentication factors.

TYPES OF AUTHENTICATION

1. Single-factor authentication (SFA) or one-factor authentication involves matching one credential to gain access to a system (i.e., a username and a password).
2. Two-factor authentication (2FA) adds a second layer of protection to your access points. Instead of just one authentication factor, 2FA requires two factors of authentication out of the three categories
3. Three-factor authentication (3FA) requires identity-confirming credentials from three separate authentication factors (i.e., one from something you know, one from something you have, and one from something you are).
4. Multi-factor authentication (MFA) refers to any process that requires two or more factors of authentication.

TYPES OF AUTHENTICATION

5. Single sign-on (SSO) authentication allows users to log in and access multiple accounts and applications using just one set of credentials.
6. one-time password (OTP) or one-time PIN (sometimes called a dynamic password) is an auto-generated password that is valid for one login session or transaction. OTP is often used for MFA.
7. Certificate-based authentication (CBA) uses a digital certificate to identify and authenticate a user, device, or machine. A digital certificate, also known as a public-key certificate, is an electronic document that stores the public key data, including information about the key, its owner, and the digital signature verifying the identity.
8. Biometric authentication relies on biometrics like fingerprints, retinal scans, and facial scans to confirm a user's identity.

DETERENT CONTROLS: REMOTE ACCESS CONTROLS

1. *Dedicated leased lines* are telephone connections that are private in the sense that the leasing telecommunications company does not allow external parties to access them.
2. *Automatic dial-back* is a control in which the remote user's computer modem dials a phone number dedicated to remote network sign-on.
3. *Secure sockets layer* is a protocol used to provide encrypted Internet sessions between remote computers and the network server.
4. *Multifactor authentication* is the implementation of two or more controls prior to granting access to a user. *Two-factor authentication* is typically applied to remote users.
5. *Virtual private networks* enable secure Internet sessions between remote computers and the network server, much like SSL. Unlike SSL, VPNs typically require special hardware and software. A VPN gateway server commonly protects the network server, and the remote computer must have the corresponding VPN client application to establish a secure channel (sometimes referred to as a tunnel) for the purpose of electronic data interchange or exchange.

DETERENT CONTROLS: REMOTE ACCESS CONTROLS

Internet Protocol Security (IPSec) has emerged as the dominant protocol standard for implementing VPNs.

The three security goals of IPSec are to provide:

1. Mechanisms for authentication, in order to reliably verify the identity of the sender
2. Mechanisms for integrity, in order to reliably determine that data has not been modified during transit from its source to its destination
3. Mechanisms for confidentiality, in order to transmit data that can be used only by its intended recipient and not by any unauthorized interceptor

DETERENT CONTROL: SYSTEM SECURITY ADMINISTRATION

System security administration is the process through which an information system is protected against unauthorized access and accidental or intentional destruction or alteration.

Procedure and training is essential in having effective security administration.