PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CC Certified in Cybersecurity

MARI GALLOWAY
AMENA JAMALI

CC Certified in Cybersecurity Cert Guide

Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, the Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to www.pearsonITcertification.com/register.
2. Enter the **print book ISBN**: 9780138200381.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at **PearsonTestPrep.com**. Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to **pearsonitp.echelp.org**.

Figure 4-2 Turnstiles (Image Credit: Serjio74/Shutterstock)

Barrier Gates

Barrier gates are typically used to regulate the flow and access of vehicle traffic entering and exiting a physical location. They use a horizontal "arm" that raises and lowers to give access, as illustrated in Figure 4-3. The arm is a physical barrier that serves as a deterrent to threat actors. Like turnstiles, these systems can be integrated with badge systems and security guards and are easy to use once installed. Implementing barrier gates is a great access control measure, but they do not provide the same level of security as a solid gate. A vehicle can be driven through the arm to gain access to the premises.

Bollards

Bollards, as illustrated in Figure 4-4, are beams or poles that control the flow and safety of pedestrian and vehicle traffic around a facility. These systems provide physical security at night or after hours while still allowing access during the day. The beams can be either movable or stationary or be raised and lowered manually or automatically using hydraulics, based on the needs of the organization. Bollards are used a lot around government buildings or places that contain highly sensitive data. The primary drawback of bollards is that they can be difficult to implement

around existing buildings due to lack of space to install them. They can also slow down emergency personnel.

Figure 4-3 Barrier Gates (Image Credit: Fedor Selivanov/Shutterstock)

Figure 4-4 Bollards (Image Credit: Ratchat/Shutterstock)

Access Control

Access to the operational controls of a gate or barrier system should be restricted to authorized personnel who need access to the gate or barrier. Often, these systems integrate with a badge system and may require an access code or PIN to verify the user is authorized to access the space or data they are trying to access. Authorized personnel can easily control, manage, and change the code within an access control system, allowing them to adjust operational controls as needed.

Biometric authentication, such as through the use of fingerprints and facial recognition, provides other ways that authorized access may be granted. Today, we have the ability to log in to smart phones, tablets, and computers with these types of authentication methods. Based on the device settings and what permissions are granted, users can gain access to facilities and data based on their unique physical characteristics. This form of authentication is great because it is hard to fake a fingerprint or someone's face when trying to gain unauthorized access, contrary to what we see in movies and TV series!

As mentioned previously, gate and barrier systems can also integrate with badging systems to synchronize access across the systems. This integration allows an employee to use their badge to gain physical access to an environment. When the badge is used, the employee's permissions are checked in real time against the database to see what level of access, if any, they should have. This also reduces the risk of unauthorized access and provides an additional layer of security.

Environmental Design

Environmental design can also play an important role in physically securing a facility. When considering the design of physical access controls, consider the Crime Prevention Through Environmental Design (CPTED) concept. CPTED is a multidisciplinary approach to crime prevention that uses environmental design strategies to deter criminal activity. An organization should consider the following four principles:

- *Natural surveillance* is using people, such as security guards, or technology, such as lighting, to observe an area. The presence of these measures keeps intruders out because they do not want to be observed.
- *Natural access control* such as bollards, landscaping, gates, and other physical features can be used to control the flow of traffic and pedestrians.
- *Territorial reinforcement* creates clear boundaries between public and private spaces, reinforcing "ownership" of the property by the authorized users.
- *Maintenance* is an ongoing task to ensure the surrounding property and the access controls in place are still effective. If an area looks outdated, threat actors might be more likely to attempt to gain access to the premises.

Following this method will allow organizations to make informed decisions about current locations and future locations when it comes to physical security.

Environmental controls also aid in the previously mentioned SPOE strategies, helping to reduce the number of physical entry points an organization's campus or building has. Having a single entry point from an environmental standpoint helps an organization strictly control the process of identifying who is and is not authorized to access the premises. This approach helps regulate entry and deters unauthorized access. In an emergency situation, bollards can be raised to stop someone from leaving without permission fairly quickly. Similarly, the SPOE strategy can prevent unauthorized personnel from leaving without first being questioned.

Key Topic

Monitoring for Physical Security

Once access controls are put in place, organizations must monitor these systems and take action if unauthorized guests gain access to the facility. Monitoring can be conducted in various ways, such as using security guards, CCTV, or reviewing the access logs.

Security Guards

In a previous life, I (Mari Galloway) was an armed ***security guard*** at the headquarters of the U.S. Department of State in Washington, DC. My job was to patrol and grant access to the State Department based on whether those entering the facility were visitors or authorized personnel.

There were multiple checks to gain access to the property and then again to access the actual building. We checked every person's identification, whether it was a smart card, driver's license, or other form of identification, and then granted access if appropriate. At the State Department, many types of barriers and gates were used, such as bollards and control arms, which both detected and prevented unauthorized access.

The role of the security guard is to patrol and monitor the premises for any signs of unauthorized access, suspicious activity, or security breaches. Guards are essentially the first line of defense when it comes to physical security and serve as a physical deterrent. They use CCTV to monitor and ensure the safety and security of the building. The use of CCTV also allows for faster threat detection. Security guards check the identification of all those entering the premises and can allow visitors into the space based on what they need and where they need to go. In addition to their surveillance duties, security guards are also trained in emergency response for fires and medical emergencies. They have a clear understanding of evacuation routes, assembly points, and emergency communications systems within the facility.

Training for security guards should be ongoing to ensure they are versed in the newest threats and monitoring techniques. Training such as live simulations should also be conducted for incident response purposes. Guards should also be trained and encouraged to build positive relationships with employees and visitors to help with information gathering should incidents or events occur. We want people to approach guards with critical issues they are observing so those concerns can be addressed promptly.

Closed-Circuit Television

A ***closed-circuit television (CCTV)*** system is a network of cameras strategically placed to monitor and record activities in and outside a facility. Several countries and cities also use this technology to monitor suspicious or illegal activity. CCTV setups can include any or all of the following camera types:

- **Fixed cameras:** Cameras that are stationary and capture a specific field of view.
- **Pan-tilt-zoom (PTZ) cameras:** Cameras that can be controlled from a control room and can be moved to get a better view of a situation.
- **Dome cameras:** Cameras that are typically used indoors and are more aesthetically pleasing.
- **Bullet cameras:** Weather-resistant cameras that are cylindrical (like bullets) and mounted on poles to provide a wide view of an area or building.

Combining all these types of cameras in a CCTV system allows an organization to have a full internal and external view of what is going on around its facility.

A networked video management system (VMS) is a combination of hardware and software components used to manage and control video surveillance cameras across different locations. VMS provides functionality such as live video viewing, camera configuration, video playback, and access control integration. Users can set up notifications for alerts, video analytics, motion detection, and more advanced options.

Where these cameras are placed is critical to the success of managing access controls. Understanding what is considered critical in an organization helps determine where cameras are placed. Ideally, cameras should be located where entry and exit points exist in a facility. These can include parking lots, high-traffic areas, places where valuable assets are stored such as vaults, and any area prone to a potential security breach such as a server room. Cameras should be placed in locations that provide the best view of the area being surveilled. They should also be out of reach to prevent tampering with or destroying the camera. Blind spots, lighting, and camera resolution all play a role in finding the best location for camera placement.

No one wants their brand-new cameras placed where the sun can obstruct the camera view, thereby causing a gap in security.

Once CCTV systems are installed, they must be monitored. Standard operating procedures (SOPs) should be in place for employees to understand what they should do if they view suspicious activity. Typically, the CCTV network is monitored by security guards who are trained in how to utilize this type of technology. Because these cameras are recording continuously, how long data is stored—data retention—is based on the legal requirements of the jurisdiction the organization falls in and organizational policies. Access to this data should also be restricted to those with a need to know and law enforcement should an incident occur.

Alarm Systems

An ***alarm system*** provides an additional layer of physical security by sounding an alert if someone tries to circumvent another physical security measure to gain access to areas they are not authorized to access. A comprehensive alarm system includes various sensors placed on doors, windows, and other access points within the organization to detect unauthorized access and alert personnel. It may also include motion detectors that send alerts when motion is detected during a time when there should not be movement.

When an alarm is triggered, organizations will activate their incident response plan to investigate and triage the alarm. Depending on the severity of the alarm, the incident response team will notify the stakeholders to jump into action. The incident response plan identifies when stakeholders should be contacted and by whom. Clearly defined incident response procedures are important to mitigate any issues in a quick and timely fashion. Security guards typically monitor these alarms and can react quickly when incidents occur. There are also offsite, remote monitoring systems that track all alerts for various organizations. Smaller organizations may use a monitoring center if they don't have personnel in-house, which allows for two-way communication between the organization and the monitoring team to verify and confirm that an event is occurring.

Logs and Documentation

Logs are generated when access is granted or denied to entry points of a facility. These logs can then be reviewed if an alarm is triggered, for further investigation. These logs, along with other network and system logs, are usually reviewed by the security operations team in a SIEM, if applicable. In smaller organizations the physical security team may review those logs when an alarm is triggered.

Access logs and entry and exit attempts create an accountability trail as they record the who, what, when, and where of the access. These logs also record failed access