user or group of users
(“new” meaning previously not available to that user or group). Technically, provisioning and

895
Configuration Management vs. Change Management
Change management is a business process aimed at deliberately regulating the changing nature of business activities such as projects or IT services. It is concerned
with issues such as changing the features in a system being developed or changing
the manner in which remote workers connect to the internal network. While IT and security personnel are involved in change management, they are usually not in
charge of it.
Configuration management is an operational process aimed at ensuring that controls are configured correctly and are responsive to the current threat and operational
environments. As an information security professional, you would likely lead in configuration management but simply participate in change management processes.

configuration are two different but related activities. Provisioning generally entails acquiring, installing, and launching a new service. Depending on how this is done, that service
may still need to be configured (and possibly even baselined).

Automation
As you can imagine, configuration management requires tracking and updating a lot
of information on many different systems. This is why mature organizations leverage
automation for many of the required tasks, including maintaining individual configuration items in a configuration management database (CMDB). The CMDB can store
information about all organizational assets, their baselines, and their relationships to one
another. Importantly, a CMDB provides versioning so that, if a configuration error is
made, reverting to a previous baseline is easy.
More elaborate automation tools are capable of not only tracking configurations but
also provisioning systems that implement them. Perhaps the best-known tool in this
regard, particularly for virtualized or cloud infrastructures, is Ansible, which is an opensource configuration management, deployment, and orchestration tool. Through the use
of playbooks written in YAML (which, recursively, stands for “YAML Ain’t Markup Language”), Ansible allows automated asset provisioning and configuration.

Resource Protection

In Chapter 5, we defined assets as anything of worth to the organization. A related concept is a resource, which is anything that is required to perform an activity or accomplish
a goal. So, a resource can also be an asset if you own it and it has inherent value to you.
In the context of security operations, a resource is anything the organization needs to
accomplish any of its tasks. This includes hardware, software, data, and the media on
which the last two are stored.

EXAM TIP Though assets and resources are, technically, slightly different things, you should treat them as synonymous in the exam.

We will discuss how to protect hardware resources later in this chapter when we cover
physical security. Though we already covered software, data, and media protections in
Chapter 6, the topic is worth revisiting as it applies to managing security operations.
There are three types of digital resources that are of particular interest in this regard:
system images, source files, and backups.

System Images

Because system images are essential to efficiently provisioning systems, they are a key
resource both during normal operations and when we are responding to a security incident. Presumably, the images we use to clone new (or replacement) systems are secure
because (as a best practice) we put a lot of work into hardening them and ensuring they
contain no known vulnerabilities. However, if adversaries were able to modify the images
so as to introduce vulnerabilities, they would have free access to any system provisioned
using the tainted images. Similarly, if the images were destroyed (deliberately, accidentally, or through an act of nature), recovering from a large-scale incident would be much
more difficult and time-consuming.

Source Files

If the images were unavailable or otherwise compromised, we would have to rebuild
everything from scratch. There are also cases in which we just need to install specific software. Either way, we need reliable source files. Source files contain the code that executes
on a computer to provide applications or services. This code can exist in either executable form or as a sequence of statements in a high-level language such as C/C++, Java, or
Python. Either way, it is possible for adversaries to insert malicious code into

source files
so that any system provisioned using them will be vulnerable. Worse yet, if you work for
a software company with clients around the world, your company may be a much more
interesting target for advanced persistent threats (APTs) who may want to compromise
your software to breach your customers. This kind of software supply-chain attack is best
exemplified by the SolarWinds attack of 2020.
Even if your organization is not likely to be targeted by APTs, you are probably concerned about ransomware attacks. Having good backups is the key to quickly recovering from ransomware (without having to pay the ransom), but it hinges on the
integrity and availability of the backup data. Many cybercriminals deliberately look for
backups and encrypt them also to force their victims to pay the ransom.

Backups
Backing up software and having backup hardware devices are two large parts of network
availability. You need to be able to restore data if a hard drive fails, a disaster takes place,
or some type of software corruption occurs.

Every organization should develop a policy that indicates what gets backed up, how
often it gets backed up, and how these processes should occur. If users have important
information on their workstations, the operations department needs to develop a method
that indicates that backups include certain directories on users’ workstations or that users
move their critical data to a server share at the end of each day to ensure it gets backed
up. Backups may occur once or twice a week, every day, or every three hours. It is up to
the organization to determine this interval. The more frequent the backups, the more
resources will be dedicated to it, so there needs to be a balance between backup costs and
the actual risk of potentially losing data.
An organization may find that conducting automatic backups through specialized software is more economical and effective than spending IT work-hours on the task. The
integrity of these backups needs to be checked to ensure they are happening as expected—
rather than finding out right after two major servers blow up that the automatic backups
were saving only temporary files.

The best way to minimize your risks due to ransomware is to have effective backups that
are beyond the reach of the cybercriminals and can quickly restore affected systems. This
means putting the greatest distance (and security controls) possible between a system

and its backups. Obviously, you should never store backups on the system itself or on
a directly connected external drive. The following are some tips on how to keep your
backups away from threat actors:

- Use a different OS for your backup server. Most ransomware today targets a single
type of OS (mostly Windows). Even if the attack is not automated, threat actors are likelier to be proficient in whatever OS they are attacking, so having your backups managed by a system running a different OS automatically gives you a leg up.
- Get your backups out of town. Whatever you do, make sure your backups are not on a drive that is directly attached to the asset you are protecting, or even on the
same LAN segment (like in the same data center). The more distance, the better, especially if you can layer controls like ACLs or even use data diodes. We know of data so sensitive that its backups are physically transported to other states or
countries periodically.
- Go old school. Consider using older technologies like optical discs and magnetic
tapes. You may get some weird looks from your early-adopter colleagues, but you may save the day when things go sideways on you.
- Protect your backups like your career depends on it. (It may!) Stay up to date on the
latest techniques cybercriminals are using to attack backups and ensure you have adequate controls in place to prevent them from being effective.

Hierarchical Storage Management

Hierarchical storage management (HSM) provides continuous online backup functionality. It combines hard disk technology with the cheaper and slower optical or tape jukeboxes. The HSM system dynamically manages the storage and recovery of files, which
are copied to storage media devices that vary in speed and cost. The faster media holds
the files that are accessed more often, and the seldom-used files are stored on the slower
devices, or near-line devices, as shown in Figure 20-1. The storage media could include

optical discs, magnetic disks, and tapes. This functionality happens in the background
without the knowledge of the user or any need for user intervention.
HSM works, according to tuning based on the trade-off between the cost of storage
and the availability of information, by migrating the actual content of less used files to
lower-speed, lower-cost storage, while leaving behind a “stub,” which looks to the user
like it contains the full data of the migrated file. When the user or an application accesses
the stub, the HSM uses the information in the stub to find the real location of the
information and then retrieve it transparently for the user.
This type of technology was created to save money and time. If all data was stored on
hard drives, that would be expensive. If a lot of the data was stored on tapes, it would
take too long to retrieve the data when needed. So HSM provides a terrific approach by
providing you with the data you need, when you need it, without having to bother the
administrator to track down some tape or optical disc.

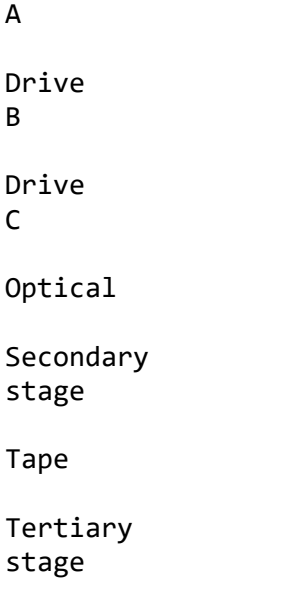


Figure 20-1

HSM provides an economical and efficient way of storing data.

Backups should include the underlying operating system and applications, as well as

the configuration files for both. Systems are attached to networks, and network devices
can experience failures and data losses as well. Data loss of a network device usually
means the configuration of the network device is lost completely (and the device will not
even boot up), or that the configuration of the network device reverts to defaults (which,
though it will boot up, does your network little good). Therefore, the configurations of
network and other nonsystem devices (for example, the phone system) in the environment
are also necessary.

Vulnerability and Patch Management

Dealing with new vulnerabilities and their corresponding patches is an inevitability in
cybersecurity. The trick is to deal with these in an informed and deliberate manner.
While the following sections treat vulnerability management and patch management
separately, it is important to consider them as two pieces of the same puzzle in real life.
We may learn of a new vulnerability for which a patch does not yet exist. Equally bad
would be applying a patch that brings down a critical business system. For these reasons
(among many others), we should manage vulnerabilities and patches in a synchronized
and coordinated manner across our organizations.

Vulnerability Management

No sufficiently complex information system can ever be completely free of
vulnerabilities. Vulnerability management is the cyclical process of identifying
vulnerabilities, determining the risks they pose to the organization, and applying security controls that bring
those risks to acceptable levels. Many people equate vulnerability management with
periodically running a vulnerability scanner against their systems, but the process must
include more than just that. Vulnerabilities exist not only in software, which is what the
scanners assess, but also in business processes and in people. Flawed business processes,
such as sharing proprietary information with parties who have not signed a nondisclosure
agreement (NDA), cannot be detected by vulnerability scanners. Nor can they detect
users who click malicious links in e-mails. What matters most is not the tool or how
often it is run, but having a formal process that looks at the organization

holistically and
is closely tied to the risk management process.
Vulnerability management is part of our risk management process. We identify the things that we have that are of value to us and the threat actors that might take
those away from us or somehow interfere with our ability to benefit from them. Then
we figure out how these actors might go about causing us losses (in other words, exploiting our vulnerabilities) and how likely these events might be. As we discussed in
Chapter 2, this gives us a good idea of our risk exposure. The next step is to decide
which of those risks we will address and how. The “how” is typically through the application of a security control. Recall that we can never bring our risk to zero,
which means we will always have vulnerabilities for which we have no effective controls. These unmitigated risks exist because we think the chance of them being
realized or their impact on the organization (or both) is low enough for the risk to be
tolerable. In other words, the cost of mitigating the risk is not worth the return on our
investment. For those risks, the best we can do is continually monitor for changes in
their likelihood or potential impact.
As you can see, vulnerability management is all about finding vulnerabilities, understanding their impact on the organization, and determining what to do about them. Since information system vulnerabilities can exist in software, processes, or people,
it is worthwhile to discuss how we implement and support vulnerability management in
each of these areas.

Software Vulnerabilities
Vulnerabilities are usually discovered by security researchers who notify vendors and give
them some time (at least two weeks) to work on a patch before the researchers make
their findings public. This is known as responsible or ethical disclosure. The Computer
Emergency Response Team Coordination Center (CERT/CC) is the main clearinghouse for vulnerability disclosures. Once a vulnerability is discovered, vulnerability scanner
vendors release plug-ins for their tools. These plug-ins are essentially simple programs
that look for the presence of one specific flaw.
NOTE Some organizations have their own in-house vulnerability research capability or can write their own plug-ins. In our discussion, we assume the more general case in which vulnerability scanning is done using third-party commercial tools whose licenses include subscriptions to vulnerability feeds and related plug-ins.

As previously mentioned, software vulnerability scanning is what most people think of
when they hear the term vulnerability management. Scanning is simply a common type
of vulnerability assessment that can be divided into four phases:
1. Prepare First, you have to determine the scope of the vulnerability assessment.
What are you testing and how? Having defined the scope, you schedule the
event and coordinate it with affected asset and process owners to ensure it won't
interfere with critical business processes. You also want to ensure you have the
latest vulnerability signatures or plug-ins for the systems you will be testing.
2. Scan For best results, the scan is automated, follows a script, and happens
outside of the regular hours of operation for the organization. This reduces the
chance that something goes unexpectedly wrong or that you overlook a system.
During the scan, it is helpful to monitor resource utilization (like CPU and
bandwidth) to ensure you are not unduly interfering with business operations.
3. Remediate In a perfect world, you don't find any of the vulnerabilities for
which you were testing. Typically, however, you find a system that somehow
slipped through the cracks, so you patch it and rescan just to be sure. Sometimes,
however, there are legitimate business reasons why a system can't be patched (at
least right away), so remediation may require deploying a compensating control
or (in the worst case) accepting the risk as is.
PART VII

4. Document This important phase is often overlooked because some
organizations rely on the reports that are automatically generated by the scanning
tools. These reports, however, don't normally include important details like why
a vulnerability may intentionally be left unpatched, the presence of compensating
controls elsewhere, or the need for more/less frequent scanning of specific systems.
Proper documentation ensures that assumptions, facts, and decisions are preserved
to inform future decisions.

Process Vulnerabilities
A process vulnerability exists whenever there is a flaw or weakness in a business process,
independent of the use of automation. For example, suppose a user account provisioning
process requires only an e-mail from a supervisor asking for an account for the new hire.
Since e-mail messages can be spoofed, a threat actor could send a fake e-mail
impersonating a real supervisor. If the system administrator creates the account and responds with
the new credentials, the adversary would now have a legitimate account with whatever

authorizations were requested.
Process vulnerabilities frequently are overlooked, particularly when they exist at the intersection of multiple departments within the organization. In the example, the account provisioning process vulnerability exists at the intersection of a business area (where the fictitious user will supposedly work), IT, and human resources.
A good way to find process vulnerabilities is to periodically review existing processes using a red team. As introduced in Chapter 18, a red team is a group of trusted individuals whose job is to look at something from an adversary's perspective. Red teaming is useful in many contexts, including identifying process vulnerabilities. The red team's task in this context would be to study the processes, understand the organization's environment, and then look for ways to violate its security policies. Ideally, red team exercises should be conducted whenever any new process is put in place. Realistically, however, these events take place much less frequently (if at all).
NOTE The term red team exercise is often used synonymously with penetration test. In reality, a red team exercise can apply to any aspect of an organization (people, processes, facilities, products, ideas, information systems) and aims to emulate the actions of threat actors seeking specific objectives. A penetration test, on the other hand, is focused on testing the effectiveness of security controls in facilities and/or information systems.

Human Vulnerabilities

By many accounts, over 90 percent of security incidents can be traced back to a member of an organization doing something they shouldn't have, maliciously or otherwise.
This implies that if your vulnerability management is focused exclusively on hardware and software systems, you may not be reducing your attack surface by much. A common approach to managing human vulnerabilities is social engineering assessments. We briefly introduced social engineering in Chapter 18 as a type of attack but return to it now as a tool in your vulnerability management toolkit.
Chris Hadnagy, one of the world's leading experts on the subject, defines social engineering as "the act of manipulating a person to take an action that may or may not be in the 'target's' best interest." A social engineering assessment involves a team of trained personnel attempting to exploit vulnerabilities in an organization's staff. This could result in targets revealing sensitive information, allowing the social engineers into restricted areas, clicking malicious links, or plugging into their computer a thumb drive laden with malware.

903
A social engineering assessment, much like its nefarious counterpart, consists of
three phases:
1. Open-source intelligence (OSINT) collection Before manipulating a target, the social engineer needs to learn as much as possible about that person. This phase is characterized by searches for personal information in social media sites;
web searches; and observation, eavesdropping, and casual conversations. Some OSINT tools allow quick searches of a large number of sources for information on specific individuals or organizations.
2. Assessment planning The social engineer could go on gathering OSINT forever but at some point (typically very quickly) will have enough information to formulate a plot to exploit one or more targets. Some people respond emotionally to certain topics, while others may best be targeted by impersonating
someone in a position of authority. The social engineer identifies the kinds of engagements, topics, and pretexts that are likeliest to work against one or more targets.
3. Assessment execution Regardless of how well planned an assessment may be, we know that no plan survives first contact. Social engineers have to think quickly on their feet and be very perceptive of their targets' states of mind and
emotions. In this phase, they engage targets through some combination of personal face-to-face, telephonic, text, or e-mail exchange and persuade them to take some action that compromises the security of the organization.

Rarely is a social engineering assessment not effective. At the end of the event,
the assessors report their findings and use them to educate the organization on how to
avoid falling for these tricks. Perhaps the most common type of assessment is in the
form of phishing, but a real human vulnerability assessment should be much more comprehensive.

Patch Management
According to NIST Special Publication 800-40, Revision 3, Guide to Enterprise Patch
Management Technologies, patch management is "the process for identifying, acquiring,
installing, and verifying patches for products and systems." Patches are software updates
intended to remove a vulnerability or defect in the software, or to provide new features
or functionality for it. Patch management is, at least in a basic way, an established part of
organizations' IT or security operations already.
One approach to patch management is to use a decentralized or unmanaged model in which each software package on each device periodically checks for updates and, if any

are available, automatically applies them. While this approach may seem like a simple

solution to the problem, it does have significant issues that could render it unacceptably
risky for an organization. Among these risks are the following:

• Credentials Installing patches typically requires users to have admin credentials,
which violates the principle of least privilege.
• Configuration management It may be difficult (or impossible) to attest to the status of every application in the organization, which makes configuration management much more difficult.
• Bandwidth utilization Having each application or service independently download the patches will lead to network congestion, particularly if there is no
way to control when this will happen.
• Service availability Servers are almost never configured to automatically update themselves because this could lead to unscheduled outages that have a negative effect on the organization.

There is almost no advantage to decentralized patch management, except that it is
better than doing nothing. The effort saved by not having management overhead is more
than balanced by the additional effort you'll have to put into responding to incidents
and solving configuration and interoperability problems. Still, there may be situations
in which it is not possible to actively manage some devices. For instance, if your users
are allowed to work from home using personal devices, then it would be difficult to
implement the centralized approach we discuss next. In such situations, the decentralized
model may be the best to take, provided you also have a way to periodically (say, each
time users connect back to the mother ship) check the status of their updates.

Centralized Patch Management

Centralized patch management is considered a best practice for security operations.
There are multiple approaches to implementing it, however, so you must carefully consider the pluses and minuses of each. The most common approaches are

• Agent based An update agent is installed on each device. This agent communicates with one or more update servers and compares available patches with software and versions on the local host, updating as needed.

• Agentless One or more hosts remotely connect to each device on the network using admin credentials and check the remote device for needed updates. A spin on this is the use of Active Directory objects in a domain controller to manage patch levels.
• Passive Depending on the fidelity that an organization requires, it may be possible to passively monitor network traffic to infer the patch levels on each networked application or service. While minimally intrusive to the end devices, this approach is also the least effective since it may not always be possible to uniquely identify software versions through their network traffic artifacts.
Regardless of the approach you take, you want to apply the patches as quickly as possible. After all, every day you delay is an extra day that your adversaries have to exploit

your vulnerabilities. The truth is that you can’t (or at least shouldn’t) always roll out the
patch as soon as it comes out. There is no shortage of reports of major outages caused by
rolling out patches without first testing their effects. Sometimes the fault lies with the
vendor, who, perhaps in its haste to remove a vulnerability, failed to properly test that the
patch wouldn’t break any other functionality of the product. Other times the patch may
be rock solid and yet have a detrimental second- or third-order effect on other systems on
your hosts or networks. This is why testing the patch before rolling it out is a good idea.
Virtualization technologies make it easier to set up a patch test lab. At a minimum,
you want to replicate your critical infrastructure (e.g., domain controller and production
servers) in this virtual test environment. Most organizations also create at least one virtual
machine (VM) that mimics each deployed operating system, with representative services
and applications.
NOTE It is often possible to mitigate the risk created by a software vulnerability using other controls, such as rules for your firewalls, intrusion detection system (IDS), or intrusion protection system (IPS). This can buy time for you to test the patches. It also acts as a compensatory control.

Whether or not you are able to test the patches before pushing them out (and you really should), it is also a good idea to patch your subnets incrementally. It may take
longer to get to all systems, but if something goes wrong, it will only affect a subset of

Reverse Engineering Patches

Zero-day exploits are able to successfully attack vulnerabilities that are not known to the software vendor or users of its software. For that reason, zero-day exploits are able to bypass the vast majority of controls such as firewalls, antimalware, and IDS/IPS. Though zero-day exploits are very powerful, they are also exceptionally hard to develop and very expensive to buy in the underground markets.

There is an easier and cheaper way for attackers to exploit recent vulnerabilities, and that is by reverse engineering the software patches that vendors push out. This approach takes advantage of the delay between a patch being available and it getting pushed to all the vulnerable computers in the organization. If the attacker can reverse engineer the patch faster than the defenders use it to update all computers, then the attacker wins. Some vendors are mitigating this threat by using code obfuscation, which, in an ironic turn of events, is a technique developed by attackers almost 30 years ago in an effort to thwart the then simple pattern-matching approach of antimalware solutions.

Even with code obfuscation, it is just a matter of time before the bad guys figure out what the vulnerability is. This puts pressure on the defenders to roll out the patches across the entire organization as quickly as possible. In this haste, organizations sometimes overlook problem indicators. Add to this a healthy application of Murphy's law and you see why it is imperative to have a way to deal with these unknowns. A rollback plan (previously discussed in the "Change Management" section of this chapter) describes the steps by which a change is reversed in order to restore functionality or integrity.

your users and services. This gradual approach to patching also serves to reduce network congestion that could result from all systems attempting to download patches at the same time. Obviously, the benefits of gradual patching need to be weighed against the additional exposure that the inherent delays will cause.

Physical Security

We already discussed physical security in Chapter 10, but our focus then was on the design of sites and facilities. The CISSP CBK breaks physical security into design, which falls under Domain 3 (Security Architecture and Engineering), and operations,

which
falls in the current Domain 7 (Security Operations). We follow the same approach here.
As with any other defensive technique, physical security should be implemented using
the defense-in-depth secure design principle. For example, before an intruder can get to
the written recipe for your company's secret barbeque sauce, she will need to climb or cut
a fence, slip by a security guard, pick a door lock, circumvent a biometric access control
reader that protects access to an internal room, and then break into the safe that holds
the recipe. The idea is that if an attacker breaks through one control layer, there will be
others in her way before she can obtain the company's crown jewels.
NOTE It is also important to have a diversity of controls. For example, if one key works on four different door locks, the intruder has to obtain only one key. Each entry should have its own individual key or authentication combination.

This defense model should work in two main modes: one mode during normal facility
operations and another mode during the time the facility is closed. When the facility is
closed, all doors should be locked with monitoring mechanisms in strategic positions to
alert security personnel of suspicious activity. When the facility is in operation, security
gets more complicated because authorized individuals need to be distinguished from
unauthorized individuals. Perimeter security controls deal with facility and personnel
access controls and with external boundary protection mechanisms. Internal security
controls deal with work area separation and personnel badging. Both perimeter and
internal security also address intrusion detection and corrective actions. The following
sections describe the elements that make up these categories.

External Perimeter Security Controls
Your first layer of defense is your external perimeter. This could be broken down into
distinct, concentric areas of increasing security. Let's consider an example taken from the
Site Security Design Guide, published by the U.S. General Services Administration (GSA)
Public Buildings Service, which is shown in Figure 20-2. In it, we see the entire site is
fenced off, which actually creates two security zones: the (external) neighborhood (zone 1)
and the standoff perimeter (zone 2). Depending on risk levels, the organization may

want to restrict site access and parking by creating a third zone. Even if the risk is fairly
low, it may be desirable to ensure that vehicles are unable to get too close to the building.

ZONE 1
NEIGHBORHOOD
ZONE 2
STANDOFF PERIMETER

BLDG

ZONE 3
SITE ACCESS AND
PARKING
ZONE 4
SITE

ZONE 5
BUILDING ENVELOPE
ZONE 6
MANAGEMENT AND BUILDING OPERATIONS

Figure 20-2 Security zones around a facility (Source:
https://www.wbdg.org/FFC/GSA/
site_security_dg.pdf)

• Control pedestrian and vehicle traffic flows
• Provide various levels of protection for different security zones
• Establish buffers and delaying mechanisms to protect against forced entry attempts
• Limit and control entry points

This protects the facility against accidents, but also against explosions. (A good rule
of thumb is to ensure there is a 200-foot standoff distance between any vehicles and
buildings.) Then there is the rest of the enclosed site (zone 4), which could include break
areas for employees, backup power plants, and anything else around the building
exterior. Finally, there’s the inside of the building, which we’ll discuss later in this chapter.
Each of these zones has its own set of requirements, which should be increasingly restrictive the closer someone gets to the building.
External perimeter security controls are usually put into place to provide one or more
of the following services:

These services can be provided by using the following control types (which are not
all-inclusive):

• Access control mechanisms Locks and keys, an electronic card access system, personnel awareness
• Physical barriers Fences, gates, walls, doors, windows, protected vents, vehicular barriers
• Intrusion detection Perimeter sensors, interior sensors, annunciation mechanisms
• Assessment Guards, surveillance cameras
• Response Guards, local law enforcement agencies
• Deterrents Signs, lighting, environmental design

Several types of perimeter protection mechanisms and controls can be put into place to protect an organization's facility, assets, and personnel. They can deter would-be intruders, detect intruders and unusual activities, and provide ways of dealing with these issues when they arise. Perimeter security controls can be natural (hills, rivers) or manmade (fencing, lighting, gates). Landscaping is a mix of the two. In Chapter 10, we explored Crime Prevention Through Environmental Design (CPTED) and how this approach is used to reduce the likelihood of crime. Landscaping is a tool employed in the CPTED method.

Sidewalks, bushes, and created paths can point people to the correct entry points, and trees and spiky bushes can be used as natural barriers. These bushes and trees should be placed such that they cannot be used as ladders or accessories to gain unauthorized access to unapproved entry points. Also, there should not be an overwhelming number of trees and bushes, which could provide intruders with places to hide. In the following sections, we look at the manmade components that can work within the landscaping design.

Fencing

Fencing can be quite an effective physical barrier. Although the presence of a fence may only delay dedicated intruders in their access attempts, it can work as a psychological deterrent by telling the world that your organization is serious about protecting itself.

Fencing can provide crowd control and helps control access to entrances and facilities.

However, fencing can be costly and unsightly. Many organizations plant bushes or trees in front of the fencing that surrounds their buildings for aesthetics and to make the

building less noticeable. But this type of vegetation can damage the fencing over time
or negatively affect its integrity. The fencing needs to be properly maintained, because
if a company has a sagging, rusted, pathetic fence, it is equivalent to telling the world
that the company is not truly serious and disciplined about protection. But a nice, shiny,
intimidating fence can send a different message—especially if the fencing is topped with
three rungs of barbed wire.
When deciding upon the type of fencing, several factors should be considered. For
example, when using metal fencing, the gauge of the metal should correlate to the types
of physical threats the organization most likely faces. After carrying out the risk analysis
(covered in Chapter 2), the physical security team should understand the probability of

enemies attempting to cut the fencing, drive through it, or climb over or crawl under it.
Understanding these threats will help the team determine the requirements for security
fencing.
The risk analysis results will also help indicate what height of fencing the organization
should implement. Fences come in varying heights, and each height provides a different
level of security:

- Fences three to four feet high only deter casual trespassers.
- Fences six to seven feet high are considered too high to climb easily.
- Fences eight feet high (possibly with strands of barbed or razor wire at the top)
deter the more determined intruder and clearly demonstrate your organization is
serious about protecting its property.

The barbed wire on top of fences can be tilted in or out, which also provides extra
protection. A prison would have the barbed wire on top of the fencing pointed in, which
makes it harder for prisoners to climb and escape. Most organizations would want the
barbed wire tilted out, making it harder for someone to climb over the fence and gain
access to the premises.
Critical areas should have fences at least eight feet high to provide the proper level of
protection. The fencing must be taut (not sagging in any areas) and securely connected
to the posts. The fencing should not be easily circumvented by pulling up its

posts.

Fencing: Gauges, Mesh Sizes, and Security
The gauge of fence wiring is the thickness of the wires used within the fence mesh.
The lower the gauge number, the larger the wire diameter:

- 11 gauge = 0.0907-inch diameter
- 9 gauge = 0.1144-inch diameter
- 6 gauge = 0.162-inch diameter

- Extremely high security 3/8-inch mesh, 11 gauge
- Very high security 1-inch mesh, 9 gauge
- High security 1-inch mesh, 11 gauge
- Greater security 2-inch mesh, 6 gauge
- Normal industrial security 2-inch mesh, 9 gauge

PART VII

The mesh sizing is the minimum clear distance between the wires. Common mesh sizes are 2 inches, 1 inch, and 3/8 inch. It is more difficult to climb or cut fencing with smaller mesh sizes, and the heavier-gauged wiring is harder to cut. The following list indicates the strength levels of the most common gauge and mesh sizes used in chain-link fencing today:

PIDAS Fencing
Perimeter Intrusion Detection and Assessment System (PIDAS) is a type of fencing that has sensors located on the wire mesh and at the base of the fence. It is used to detect if someone attempts to cut or climb the fence. It has a passive cable vibration sensor that sets off an alarm if an intrusion is detected. PIDAS is very sensitive and can cause many false alarms.

The posts should be buried sufficiently deep in the ground and should be secured with concrete to ensure they cannot be dug up or tied to vehicles and extracted. If the ground is soft or uneven, this might provide ways for intruders to slip or dig under the fence. In these situations, the fencing should actually extend into the dirt to thwart these types of attacks.
Fences work as “first line of defense” mechanisms. A few other controls can be used also.
Strong and secure gates need to be implemented. It does no good to install a

highly fortified
and expensive fence and then have an unlocked or flimsy gate that allows easy access.
Gates basically have four distinct classifications:

• Class I Residential usage
• Class II Commercial usage, where general public access is expected; examples include a public parking lot entrance, a gated community, or a self-storage facility
• Class III Industrial usage, where limited access is expected; an example is a warehouse property entrance not intended to serve the general public
• Class IV Restricted access; this includes a prison entrance that is monitored either in person or via closed circuitry

Each gate classification has its own long list of implementation and maintenance guidelines to ensure the necessary level of protection. These classifications and guidelines
are developed by UL (formerly Underwriters Laboratory), a nonprofit organization that
tests, inspects, and classifies electronic devices, fire protection equipment, and specific
construction materials. This is the group that certifies these different items to ensure they
are in compliance with national building codes. A specific UL code, UL 325, deals with
garage doors, drapery, gates, and louver and window operators and systems.
So, whereas in the information security world we look to NIST for our best practices
and industry standards, in the physical security world, we look to UL for the same type
of direction.

Bollards
Bollards usually look like small concrete pillars outside a building. Sometimes companies
try to dress them up by putting flowers or lights in them to soften the look of a protected
environment. They are placed by the sides of buildings that have the most immediate
threat of someone driving a vehicle through the exterior wall. They are usually placed

between the facility and a parking lot and/or between the facility and a road that runs
close to an exterior wall. An alternative, particularly in more rural environments, is to use
very large boulders to surround and protect sensitive sites. They provide the same type of
protection that bollards provide.

Lighting
Many of the items mentioned in this chapter are things people take for granted

day in
and day out during our usual busy lives. Lighting is certainly one of those items you
probably wouldn’t give much thought to, unless it wasn’t there. Unlit (or improperly lit)
parking lots and parking garages have invited many attackers to carry out
criminal activity that they may not have engaged in otherwise with proper lighting. Breaking into cars,
stealing cars, and attacking employees as they leave the office are the more common types
of attacks that take place in such situations. A security professional should understand
that the right illumination needs to be in place, that no dead spots (unlit areas) should
exist between the lights, and that all areas where individuals may walk should be properly
lit. A security professional should also understand the various types of lighting available
and where they should be used.
Wherever an array of lights is used, each light covers its own zone or area. The size of
the zone each light covers depends on the illumination of light produced, which usually
has a direct relationship to the wattage capacity of the bulbs. In most cases, the higher
the lamp’s wattage, the more illumination it produces. It is important that the zones of
illumination coverage overlap. For example, if a company has an open parking lot, then
light poles must be positioned within the correct distance of each other to eliminate any
dead spots. If the lamps that will be used provide a 30-foot radius of illumination, then
the light poles should be erected less than 30 feet apart so there is an overlap between the
areas of illumination.
NOTE Critical areas need to have illumination that reaches at least eight feet with the illumination of two foot-candles. Foot-candle is a unit of measure of the intensity of light.

PART VII

If an organization does not implement the right types of lights and ensure they provide
proper coverage, the probability of criminal activity, accidents, and lawsuits increases.
Exterior lights that provide protection usually require less illumination intensity than
interior working lighting, except for areas that require security personnel to inspect
identification credentials for authorization. It is also important to have the correct
lighting when using various types of surveillance equipment. The correct contrast

between a potential intruder and background items needs to be provided, which only
happens with the correct illumination and placement of lights. If the light is going to
bounce off of dark, dirty, or darkly painted surfaces, then more illumination is required
for the necessary contrast between people and the environment. If the area has clean
concrete and light-colored painted surfaces, then not as much illumination is required.
This is because when the same amount of light falls on an object and the surrounding
background, an observer must depend on the contrast to tell them apart.

When lighting is installed, it should be directed toward areas where potential intruders
would most likely be coming from and directed away from the security force posts. For
example, lighting should be pointed at gates or exterior access points, and the guard
locations should be more in the shadows, or under a lower amount of illumination. This
is referred to as glare protection for the security force. If you are familiar with military
operations, you might know that when you are approaching a military entry point, there
is a fortified guard building with lights pointing toward the oncoming cars. A large sign
instructs you to turn off your headlights, so the guards are not temporarily blinded by
your lights and have a clear view of anything coming their way.
Lights used within the organization’s security perimeter should be directed outward,
which keeps the security personnel in relative darkness and allows them to easily view
intruders beyond the organization’s perimeter.
An array of lights that provides an even amount of illumination across an area is usually
referred to as continuous lighting. Examples are the evenly spaced light poles in a parking
lot, light fixtures that run across the outside of a building, or a series of fluorescent lights
used in parking garages. If an organization’s building is relatively close to someone else’s
developed property, a railway, an airport, or a highway, the organization may need to
ensure the lighting does not “bleed over” property lines in an obtrusive manner. Thus,
the illumination needs to be controlled, which just means the organization should erect
lights and use illumination in such a way that it does not blind its neighbors

or any
passing cars, trains, or planes.
You probably are familiar with the special home lighting gadgets that turn certain
lights on and off at predetermined times, giving the illusion to potential burglars that
a house is occupied even when the residents are away. Organizations can use a similar
technology, which is referred to as standby lighting. The security personnel can configure
the times that different lights turn on and off, so potential intruders think different areas
of the facility are populated.
NOTE Redundant or backup lights should be available in case of power failures or emergencies. Special care must be given to understand what type of lighting is needed in different parts of the facility in these types of situations. This lighting may run on generators or battery packs.

Responsive area illumination takes place when an IDS detects suspicious activities and
turns on the lights within a specific area. When this type of technology is plugged into
automated IDS products, there is a high likelihood of false alarms. Instead of continually
having to dispatch a security guard to check out these issues, an organization can install a
CCTV camera (described in the upcoming section “Visual Recording Devices”) to scan
the area for intruders.
If intruders want to disrupt the security personnel or decrease the probability of being
seen while attempting to enter an organization’s premises or building, they could attempt
to turn off the lights or cut power to them. This is why lighting controls and switches
should be in protected, locked, and centralized areas.

Surveillance Devices
Usually, installing fences and lights does not provide the necessary level of protection an
organization needs to protect its facility, equipment, and employees. Therefore, an organization needs to ensure that all areas are under surveillance so that security personnel
notice improper actions and address them before damage occurs. Surveillance can happen through visual detection or through devices that use sophisticated means of detecting abnormal behavior or unwanted conditions. It is important that every organization
have a proper mix of lighting, security personnel, IDSs, and surveillance technologies
and techniques.

Visual Recording Devices

Because surveillance is based on sensory perception, surveillance devices usually work in conjunction with guards and other monitoring mechanisms to extend their capabilities and range of perception. A closed-circuit TV (CCTV) system is a commonly used monitoring device in most organizations, but before purchasing and implementing a CCTV system, you need to consider several items:

- The purpose of CCTV To detect, assess, and/or identify intruders
- The type of environment the CCTV camera will work in Internal or external areas
- The field of view required Large or small area to be monitored
- Amount of illumination of the environment Lit areas, unlit areas, areas affected by sunlight
- Integration with other security controls Guards, IDSs, alarm systems

PART VII

The reason you need to consider these items before you purchase a CCTV product is that there are so many different types of cameras, lenses, and monitors that make up the different CCTV products. You must understand what is expected of this physical security control, so that you purchase and implement the right type.

CCTVs are made up of cameras, a controller and digital video recording (DVR) system, and a monitor. Remote storage and remote client access are usually added to prevent threat actors (criminals, fire) from destroying the recorded videos and to allow off-duty staff to report to alarms generated by the system without having to drive back to the office. The camera captures the data and transmits it to the controller, which allows the data to be displayed on a local monitor. The data is recorded so that it can be reviewed at a later time if needed. Figure 20-3 shows how multiple cameras can be connected to one controller, which allows several different areas to be monitored at one time. The controller accepts video feed from all the cameras and interleaves these transmissions over one line to the central monitor.

A CCTV sends the captured data from the cameras to the controller using a special network, which can be wired or wireless. The term “closed-circuit” comes from the fact that the very first systems used this special closed network instead of broadcasting the signals over a public network. This network should be encrypted so that an intruder

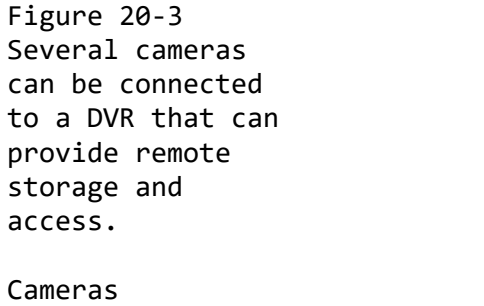


Figure 20-3
Several cameras
can be connected
to a DVR that can
provide remote
storage and
access.

cannot manipulate the video feed that the security guard is monitoring. The most common type of attack is to replay previous recordings without the security personnel knowing it. For example, if an attacker is able to compromise a company's CCTV and play the recording from the day before, the security guard would not know an intruder is in the facility carrying out some type of crime. This is one reason why CCTVs should be used in conjunction with intruder detection controls, which we address in the next section.

Most of the CCTV cameras in use today employ light-sensitive chips called chargedcoupled devices (CCDs). The CCD is an electrical circuit that receives input light from the lens and converts it into an electronic signal, which is then displayed on the monitor.

Images are focused through a lens onto the CCD chip surface, which forms the electrical representation of the optical image. It is this technology that allows for the capture of extraordinary detail of objects and precise representation, because it has sensors that work in the infrared range, which extends beyond human perception. The CCD sensor picks up this extra "data" and integrates it into the images shown on the monitor to allow for

better granularity and quality in the video.
Two main types of lenses are used in CCTV: fixed focal length and zoom (varifocal).
The focal length of a lens defines its effectiveness in viewing objects from a horizontal and vertical view. The focal length value relates to the angle of view that can be achieved.
Short focal length lenses provide wider-angle views, while long focal length lenses provide a narrower view. The size of the images shown on a monitor, along with the area covered by one camera, is defined by the focal length. For example, if a company implements a CCTV camera in a warehouse, the focal length lens values should be between 2.8 and 4.3 millimeters (mm) so the whole area can be captured. If the company implements another CCTV camera that monitors an entrance, that lens value should be around 8 mm, which allows a smaller area to be monitored.

NOTE Fixed focal length lenses are available in various fields of views: wide, medium, and narrow. A lens that provides a “normal” focal length creates a picture that approximates the field of view of the human eye. A wide-angle lens has a short focal length, and a telephoto lens has a long focal length. When an organization selects a fixed focal length lens for a particular view of an environment, it should understand that if the field of view needs to be changed (wide to narrow), the lens must be changed.

So, if we need to monitor a large area, we use a lens with a smaller focal length value.
Great, but what if a security guard hears a noise or thinks she sees something suspicious?
A fixed focal length lens does not allow the user to optically change the area that fills the monitor. Though digital systems exist that allow this change to happen in logic, the resulting image quality is decreased as the area being studied becomes smaller. This is because the logic circuits are, in effect, cropping the broader image without increasing the number of pixels in it. This is called digital zoom (as opposed to optical zoom) and is a common feature in many cameras. The optical zoom lenses provide flexibility by allowing the viewer to change the field of view while maintaining the same number of pixels in the resulting image, which makes it much more detailed. The security personnel usually

have a remote-control component integrated within the centralized CCTV monitoring area that allows them to move the cameras and zoom in and out on objects as needed.

When both wide scenes and close-up captures are needed, an optical zoom lens is best.

To understand the next characteristic, depth of field, think about pictures you might take while on vacation with your family. For example, if you want to take a picture of your spouse with the Grand Canyon in the background, the main object of the picture is your spouse. Your camera is going to zoom in and use a shallow depth of focus. This provides a softer backdrop, which will lead the viewers of the photograph to the foreground, which is your spouse. Now, let's say you get tired of taking pictures of your spouse and want to get a scenic picture of just the Grand Canyon itself. The camera would use a greater depth of focus, so there is not such a distinction between objects in the foreground and background.

The depth of field is necessary to understand when choosing the correct lenses and configurations for your organization's CCTV. The depth of field refers to the portion of the environment that is in focus when shown on the monitor. The depth of field varies depending on the size of the lens opening, the distance of the object being focused on, and the focal length of the lens. The depth of field increases as the size of the lens opening decreases, the subject distance increases, or the focal length of the lens decreases. So, if you want to cover a large area and not focus on specific items, it is best to use a wideangle lens and a small lens opening.

CCTV lenses have irises, which control the amount of light that enters the lens. Manual iris lenses have a ring around the CCTV lens that can be manually turned and controlled.

A lens with a manual iris would be used in areas that have fixed lighting, since the iris cannot self-adjust to changes of light. An auto iris lens should be used in environments where the light changes, as in an outdoor setting. As the environment brightens, this is sensed by the iris, which automatically adjusts itself. Security personnel will configure

the CCTV to have a specific fixed exposure value, which the iris is responsible

for
maintaining. On a sunny day, the iris lens closes to reduce the amount of light entering
the camera, while at night, the iris opens to capture more light—just like our eyes.
When choosing the right CCTV for the right environment, you must determine the amount of light present in the environment. Different CCTV camera and lens products
have specific illumination requirements to ensure the best quality images possible. The
illumination requirements are usually represented in the lux value, which is a metric used to
represent illumination strengths. The illumination can be measured by using a light meter.
The intensity of light (illumination) is measured and represented in measurement units
of lux or foot-candles. (The conversion between the two is one foot-candle = 10.76 lux.)
The illumination measurement is not something that can be accurately provided by the
vendor of a light bulb, because the environment can directly affect the illumination.
This is why illumination strengths are most effectively measured where the light source
is implemented.
Next, you need to consider the mounting requirements of the CCTV cameras. The cameras can be implemented in a fixed mounting or in a mounting that allows the cameras
to move when necessary. A fixed camera cannot move in response to security personnel
commands, whereas cameras that provide PTZ capabilities can pan, tilt, or zoom (PTZ)
as necessary. Either way, there is deterrence value in ensuring the cameras (or at least
some of them) are visible. You should also place signs stating that everyone in the area
is being monitored through CCTV. Threat actors may be less likely to engage in illicit
behavior if they know they’re being recorded on video doing so.
NOTE You should be mindful of the privacy implications of camera placement. Areas like restrooms, locker rooms, and medical exam rooms are examples of places where you should not install cameras unless you are certain you comply with all applicable laws, regulations, and ethical standards.

Now, it would be nice if someone actually watched the monitors for suspicious activities. Realizing that monitor watching is a mentally deadening activity may lead your
team to implement a type of annunciator system. Different types of annunciator products
are available that can either “listen” for noise and activate electrical devices, such as lights,
sirens, or CCTV cameras, or detect movement. Instead of expecting a security guard to

stare at a CCTV monitor for eight hours straight, the guard can carry out other activities
and be alerted by an annunciator if movement is detected on a screen.

Facility Access Control
Access control needs to be enforced through physical and technical components when it
comes to physical security. Physical access controls use mechanisms to identify individuals who are attempting to enter a facility or area. They make sure the right individuals get
in and the wrong individuals stay out and provide an audit trail of these actions. Having
personnel within sensitive areas is one of the best security controls because they can personally detect suspicious behavior. However, they need to be trained on what activity is
considered suspicious and how to report such activity.

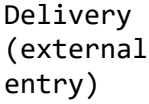
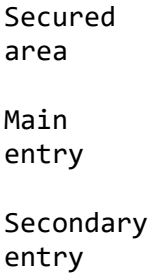


Figure 20-4
Access control
points should
be identified,
marked, and
monitored
properly.



Before an organization can put into place the proper protection mechanisms, it needs to conduct a detailed review to identify which individuals should be allowed into
what areas. Access control points can be identified and classified as external, main, and
secondary entrances. Personnel should enter and exit through a specific entry, deliveries
should be made to a different entry, and sensitive areas should be restricted. Figure 20-4
illustrates the different types of access control points into a facility. After an organization
has identified and classified the access control points, the next step is to determine how

to protect them.

Locks

PART VII

Locks are inexpensive access control mechanisms that are widely accepted and used.
They are considered delaying devices to intruders. The longer it takes to break or pick a
lock, the longer a security guard or police officer has to arrive on the scene if the intruder
has been detected. Almost any type of a door can be equipped with a lock, but keys
can be easily lost and duplicated, and locks can be picked or broken. If an organization
depends solely on a lock-and-key mechanism for protection, an individual who has the
key can come and go as he likes without control and can remove items from the premises
without detection. Locks should be used as part of the protection scheme, but should not
be the sole protection scheme.
Locks vary in functionality. Padlocks can be used on chained fences, preset locks are
usually used on doors, and programmable locks (requiring a combination to unlock)
are used on doors or vaults. Locks come in all types and sizes. It is important to have the
right type of lock so it provides the correct level of protection.
To the curious mind or a determined thief, a lock can be considered a little puzzle to
solve, not a deterrent. In other words, locks may be merely a challenge, not necessarily
something to stand in the way of malicious activities. Thus, you need to make the challenge
difficult, through the complexity, strength, and quality of the locking mechanisms.

NOTE The delay time provided by the lock should match the penetration resistance of the surrounding components (door, door frame, hinges). A smart thief takes the path of least resistance, which may be to pick the lock, remove the pins from the hinges, or just kick down the door.

Mechanical Locks Two main types of mechanical locks are available: the warded lock
and the tumbler lock. The warded lock is the basic padlock, as shown in Figure 20-5.
It has a spring-loaded bolt with a notch cut in it. The key fits into this notch and slides
the bolt from the locked to the unlocked position. The lock has wards in it,

which are
metal projections around the keyhole, as shown in Figure 20-6. The correct key for a
specific warded lock has notches in it that fit in these projections and a notch to slide
the bolt back and forth. These are the cheapest locks, because of their lack of any real
sophistication, and are also the easiest to pick.
The tumbler lock has more pieces and parts than a ward lock. As shown in Figure 20-7,
the key fits into a cylinder, which raises the lock metal pieces to the correct height so the
bolt can slide to the locked or unlocked position. Once all of the metal pieces are at the
correct level, the internal bolt can be turned. The proper key has the required size and
sequences of notches to move these metal pieces into their correct position.
The three types of tumbler locks are the pin tumbler, wafer tumbler, and lever tumbler.
The pin tumbler lock, shown in Figure 20-7, is the most commonly used tumbler lock.
The key has to have just the right grooves to put all the spring-loaded pins in the right
position so the lock can be locked or unlocked.

Figure 20-5
A warded lock

Figure 20-6
A key fits into a
notch to turn the
bolt to unlock
the lock.
Locking
bolt

Wards

Wafer tumbler locks (also called disc tumbler locks) are the small, round locks you usually
see on file cabinets. They use flat discs (wafers) instead of pins inside the locks. They
often are used as car and desk locks. This type of lock does not provide much protection
because it can be easily circumvented.
Spring

Figure 20-7
Tumbler lock
Driver
Pin

Cylinder

PART VII

Key

NOTE Some locks have interchangeable cores, which allow for the core of the lock to be taken out. You would use this type of lock if you wanted one key to open several locks. You would just replace all locks with the same core.

Combination locks, of course, require the correct combination of numbers to unlock them.
These locks have internal wheels that have to line up properly before being unlocked. A user
spins the lock interface left and right by so many clicks, which lines up the internal wheels.
Once the correct turns have taken place, all the wheels are in the right position for the lock to
release and open the door. The more wheels within the locks, the more protection provided.
Electronic combination locks do not use internal wheels, but rather have a keypad that
allows a person to type in the combination instead of turning a knob with a combination
faceplate. An example of an electronic combination lock is shown in Figure 20-8.
Cipher locks, also known as programmable locks, are keyless and use keypads to control
access into an area or facility. The lock requires a specific combination to be entered into the
keypad and possibly a swipe card. Cipher locks cost more than traditional locks, but their
combinations can be changed, specific combination sequence values can be locked out, and
personnel who are in trouble or under duress can enter a specific code that will open the door
and initiate a remote alarm at the same time. Thus, compared to traditional locks, cipher
locks can provide a much higher level of security and control over who can access a facility.
The following are some functionalities commonly available on many cipher combination
locks that improve the performance of access control and provide for increased security
levels:

• Door delay If a door is held open for a given time, an alarm triggers to alert personnel of suspicious activity.
• Key override A specific combination can be programmed for use in emergency situations to override normal procedures or for supervisory overrides.
• Master keying Supervisory personnel can change access codes and other

features of the cipher lock.
• Hostage alarm If an individual is under duress and/or held hostage, a combination
he enters can communicate this situation to the guard station and/or police station.
Figure 20-8
An electronic
combination lock

If a door is accompanied by a cipher lock, it should have a corresponding visibility
shield so a bystander cannot see the combination as it is keyed in. Automated cipher
locks must have a backup battery system and be set to unlock during a power failure so
personnel are not trapped inside during an emergency. Fail safe systems are those that are
designed and configured to ensure the safety of humans in the event of failure. Contrast
this principle with fail secure, which we discussed in Chapter 9. These two imperatives
(safety versus security) must be carefully balanced, while keeping in mind that human
safety must always be the highest priority.
CAUTION It is important to change the combination of locks and to use random combination sequences. Often, people do not change their combinations or clean the keypads, which allows an intruder to know what key values are used in the combination, because they are the dirty and worn keys. The intruder then just needs to figure out the right combination of these values.

Some cipher locks require all users to know and use the same combination, which does not allow for any individual accountability. Some of the more sophisticated cipher
locks permit specific codes to be assigned to unique individuals. This provides more
accountability, because each individual is responsible for keeping his access code secret,
and entry and exit activities can be logged and tracked. These are usually referred to
as smart locks, because they are designed to allow only authorized individuals access at
certain doors at certain times.
NOTE Hotel key cards are also known as smart cards. The access code on the card can allow access to a hotel room, workout area, business area, and better yet—the mini bar.

Device Locks Unfortunately, hardware has a tendency to “walk away” from facilities;
thus, device locks are necessary to thwart these attempts. Cable locks consist
of a vinylcoated steel cable that can secure a computer or peripheral to a desk

or other stationary
components, as shown in Figure 20-9.
The following are some of the device locks available and their capabilities:

• Switch controls Cover on/off power switches
• Slot locks Secure the system to a stationary component by the use of steel cable
that is connected to a bracket mounted in a spare expansion slot
• Port controls Block access to disk drives or unused serial or parallel ports
• Peripheral switch controls Secure a keyboard by inserting an on/off switch between the system unit and the keyboard input slot
• Cable traps Prevent the removal of input/output devices by passing their cables
through a lockable unit

Figure 20-9
Laptop security
cable kits secure
a computer by
enabling the
user to attach
the device to
a stationary
component
within an area.

Administrative Responsibilities It is important for an organization not only to choose the right type of lock for the right purpose but also to follow proper maintenance
and procedures. Keys should be assigned by facility management, and this assignment
should be documented. Procedures should be written out detailing how keys are to be
assigned, inventoried, and destroyed when necessary and what should happen if and
when keys are lost. Someone on the organization’s facility management team should be
assigned the responsibility of overseeing key and combination maintenance.
Most organizations have master keys and submaster keys for the facility management
staff. A master key opens all the locks within the facility, and the submaster keys open
one or more locks. Each lock has its own individual unique keys as well. So if a facility
has 100 offices, the occupant of each office can have his or her own key. A master key
allows access to all offices for security personnel and for emergencies. If one security
guard is responsible for monitoring half of the facility, the guard can be

assigned one of
the submaster keys for just those offices.
Since these master and submaster keys are powerful, they must be properly guarded
and not widely shared. A security policy should outline what portions of the facility and
which device types need to be locked. As a security professional, you should understand
what type of lock is most appropriate for each situation, the level of protection provided
by various types of locks, and how these locks can be circumvented.
Circumventing Locks Each lock type has corresponding tools that can be used to pick it (open it without the key). A tension wrench is a tool shaped like an L and is
used to apply tension to the internal cylinder of a lock. The lock picker uses a lock
pick to manipulate the individual pins to their proper placement. Once certain pins are
“picked” (put in their correct place), the tension wrench holds these down while the lock
picker figures out the correct settings for the other pins. After the intruder determines the
proper pin placement, the wrench is used to then open the lock.
Intruders may carry out another technique, referred to as raking. To circumvent a pin
tumbler lock, a lock pick is pushed to the back of the lock and quickly slid out while
providing upward pressure. This movement makes many of the pins fall into place. A
tension wrench is also put in to hold the pins that pop into the right place. If all the pins
do not slide to the necessary height for the lock to open, the intruder holds the tension
wrench and uses a thinner pick to move the rest of the pins into place.

Lock Strengths
Basically, three grades of locks are available:

• Grade 1 Commercial and industrial use
• Grade 2 Heavy-duty residential/light-duty commercial
• Grade 3 Residential/consumer
The cylinders within the locks fall into three main categories:

• Low security No pick or drill resistance provided (can fall within any of the three grades of locks)
• Medium security A degree of pick-resistance protection provided (uses tighter and more complex keyways [notch combination]; can fall within any of the three grades of locks)
• High security Pick-resistance protection through many different mechanisms (only used in grade 1 and 2 locks)

To resist drilling, hardened steel inserts are
added to critical sections of the lock face
and sidebar.
Keys require special cutting
machines to precisely duplicate
the right, left, and center angles.

Pick-resistant pin
tumbler must be
elevated and rotated
to the proper
position for the lock
cylinder to operate.

Secondary sidebar locking mechanism can only
operate when tumblers are properly aligned.

The common lock cylinder, with no hardened steel
inserts,offers little protection against drilling.

PART VII

A common key can be created
and has no provision for
controlled duplication.

Common pin
tumblers are
vulnerable to
picking.

Lock bumping is a tactic that intruders can use to force the pins in a tumbler lock to
their open position by using a special key called a bump key. The stronger the material that
makes up the lock, the smaller the chance that this type of lock attack will be successful.
Now, if this is all too much trouble for the intruder, she can just drill the lock, use bolt
cutters, attempt to break through the door or the doorframe, or remove the hinges. There
are just so many choices for the bad guys.

Internal Security Controls
The physical security controls we've discussed so far have been focused on the perimeter.
It is also important, however, to implement and manage internal security controls to
mitigate risks when threat actors breach the perimeter or are insider threats. One type of
control we already discussed in Chapter 10 is work area separation, in which we

create
internal perimeters around sensitive areas. For example, only designated IT and security personnel should be allowed in the server room. Access to these areas can then be
restricted using locks and self-closing doors.
When implementing work area separation, we can start with a concentric zone model
similar to the one we used for the external perimeter. Most staff will probably be able to
move freely across the largest zone so that they can do their jobs. This general zone would
have some controls, but not a bunch of them. Some staff members will also be allowed
to go into more sensitive areas such as the operations center and the executive suite.
These areas require some sort of access control like swiping a badge, but they're generally
staffed so the people working there act as a sort of intrusion detection system when they
see someone who doesn't belong. There can also be a highly sensitive zone that includes
spaces where you really can't have any unauthorized persons, particularly if the spaces
are not always staffed. Examples of these highly sensitive areas are server rooms, narcotic
storage spaces (in healthcare facilities), and hazardous materials storerooms.
Physical security teams could include roving guards that move around the facility
looking for potential security violations and unauthorized personnel. These teams could
also monitor internal security cameras and be trained on how to respond to incidents
such as medical emergencies and active shooters.

Personnel Access Controls
Proper identification verifies whether the person attempting to access a facility or area
should actually be allowed in. Identification and authentication can be verified by matching an anatomical attribute (biometric system), using smart or memory cards (swipe
cards), presenting a photo ID to a security guard, using a key, or providing a card and
entering a password or PIN.
Personnel should be identified with badges that must be worn visibly while in the
facility. The badges could include a photo of the individual and be color-coded to show
clearance level, department, and whether or not that person is allowed to escort visitors.
Visitors could be issued temporary badges that clearly identify them as such. All personnel
would be trained to challenge anyone walking around without a badge or call security
personnel to deal with them.

A common problem with controlling authorized access into a facility or area is called piggybacking. This occurs when an individual gains unauthorized access by using someone else's legitimate credentials or access rights. Usually, an individual just follows another person closely through a door without providing any credentials. The best preventive measures against piggybacking are to have security guards at access points and to educate employees about good security practices.

If an organization wants to use a card badge reader, it has several types of systems to choose from. Most systems are based on issuing to personnel cards that have embedded magnetic strips that contain access information. The reader can just look for simple access information within the magnetic strip, or it can be connected to a more sophisticated system that scans the information, makes more complex access decisions, and logs badge IDs and access times.

If the card is a memory card, then the reader just pulls information from it and makes an access decision. If the card is a smart card, the individual may be required to enter a PIN or password, which the reader compares against the information held within the card or in an authentication server.

These access cards can be used with user-activated readers, which just means the user actually has to do something—swipe the card or enter a PIN. System sensing access control readers, also called transponders, recognize the presence of an approaching object within a specific area. This type of system does not require the user to swipe the card through the reader. The reader sends out interrogating signals and obtains the access code from the card without the user having to do anything.

EXAM TIP Electronic access control (EAC) tokens is a generic term used to describe proximity authentication devices, such as proximity readers, programmable locks, or biometric systems, which identify and authenticate users before allowing them entrance into physically controlled areas.

Intrusion Detection Systems

Surveillance techniques are used to watch an area, whereas intrusion detection

devices are
used to sense changes that take place in an environment. Both are monitoring methods,
but they use different devices and approaches. This section addresses the types of technologies that can be used to detect the presence of an intruder. One such technology, a
perimeter scanning device, is shown in Figure 20-10.
IDSs are used to detect unauthorized entries and to alert a responsible entity to respond.
These systems can monitor entries, doors, windows, devices, or removable coverings of
equipment. Many work with magnetic contacts or vibration-detection devices that are
sensitive to certain types of changes in the environment. When a change is detected, the
IDS device sounds an alarm either in the local area or in both the local area and a remote
police or guard station.

Figure 20-10
Different
perimeter
scanning devices
work by covering
a specific area.

IDSs can be used to detect changes in the following:

- Beams of light
- Sounds and vibrations
- Motion
- Different types of fields (microwave, ultrasonic, electrostatic)
- Electrical circuit

IDSs can be used to detect intruders by employing electromechanical systems (magnetic switches, metallic foil in windows, pressure mats) or volumetric systems.
Volumetric systems are more sensitive because they detect changes in subtle environmental
characteristics, such as vibration, microwaves, ultrasonic frequencies, infrared values, and
photoelectric changes.
Electromechanical systems work by detecting a change or break in a circuit. The electrical
circuits can be strips of foil embedded in or connected to windows. If the window breaks,
the foil strip breaks, which sounds an alarm. Vibration detectors can detect movement
on walls, screens, ceilings, and floors when the fine wires embedded within the structure
are broken. Magnetic contact switches can be installed on windows and doors. If the

contacts are separated because the window or door is opened, an alarm sounds. Another type of electromechanical detector is a pressure pad. This is placed underneath a rug or portion of the carpet and is activated after hours. If someone steps on the pad, an alarm is triggered.

A photoelectric system, or photometric system, detects the change in a light beam and thus can be used only in windowless rooms. These systems work like photoelectric smoke

detectors, which emit a beam that hits the receiver. If this beam of light is interrupted, an alarm sounds. The beams emitted by the photoelectric cell can be cross-sectional and can be invisible or visible beams. Cross-sectional means that one area can have several different light beams extending across it, which is usually carried out by using hidden mirrors to bounce the beam from one place to another until it hits the light receiver. These are the systems commonly depicted in movies. You have probably seen James Bond and other noteworthy movie spies or criminals use night-vision goggles to see the invisible beams and then step over them.

A passive infrared (PIR) system identifies the changes of heat waves in an area it is configured to monitor. If the particles' temperature within the air rises, it could be an indication of the presence of an intruder, so an alarm is sounded.

An acoustical detection system uses microphones installed on floors, walls, or ceilings. The goal is to detect any sound made during a forced entry. Although these systems are easily installed, they are very sensitive and cannot be used in areas open to sounds of storms or traffic. Vibration sensors are similar and are also implemented to detect forced entry. Financial institutions may choose to implement these types of sensors on exterior walls, where bank robbers may attempt to drive a vehicle through. They are also commonly used around the ceiling and flooring of vaults to detect someone trying to make an unauthorized bank withdrawal.

Wave-pattern motion detectors differ in the frequency of the waves they monitor. The

different frequencies are microwave, ultrasonic, and low frequency. All of these devices
generate a wave pattern that is sent over a sensitive area and reflected back to a receiver.
If the pattern is returned undisturbed, the device does nothing. If the pattern returns
altered because something in the room is moving, an alarm sounds.
A proximity detector, or capacitance detector, emits a measurable magnetic field. The
detector monitors this magnetic field, and an alarm sounds if the field is disrupted.
These devices are usually used to protect specific objects (e.g., artwork, cabinets, or a
safe) versus protecting a whole room or area. Capacitance change in an electrostatic field
can be used to catch a bad guy, but first you need to understand what capacitance change
means. An electrostatic IDS creates an electrostatic magnetic field, which is just an electric
field associated with static electric charges. Most objects have a measurable static electric
charge. They are all made up of many subatomic particles, and when everything is stable
and static, these particles constitute one holistic electric charge. This means there is a
balance between the electric capacitance and inductance. Now, if an intruder enters the
area, his subatomic particles will mess up this lovely balance in the electrostatic field,
causing a capacitance change, and an alarm will sound. So if you want to rob a company
that uses these types of detectors, leave the subatomic particles that make up your body
at home.
The type of motion detector that an organization chooses to implement, its power
capacity, and its configurations dictate the number of detectors needed to cover a
sensitive area. Also, the size and shape of the room and the items within the room may
cause barriers, in which case more detectors would be needed to provide the necessary
level of coverage.

Intrusion Detection Systems Characteristics

IDSs are very valuable controls to use in every physical security program, but several
issues need to be understood before implementing them:

- They are expensive and require human intervention to respond to the alarms.
- They require a redundant power supply and emergency backup power.
- They can be linked to a centralized security system.

- They should have a fail-safe configuration, which defaults to “activated.”
- They should detect, and be resistant to, tampering.

IDSs are support mechanisms intended to detect and announce an attempted intrusion. They will not prevent or apprehend intruders, so they should be seen as an aid to the organization’s security forces.

Patrol Force and Guards

One of the best intrusion detection mechanisms is a security guard and/or a patrol force to monitor a facility’s grounds. This type of security control is more flexible than other security mechanisms, provides good response to suspicious activities, and works as a great deterrent. However, it can be a costly endeavor because it requires a salary, benefits, and time off. People sometimes are unreliable. Screening and bonding is an important part of selecting a security guard, but this only provides a certain level of assurance. One issue is if the security guard decides to make exceptions for people who do not follow the organization’s approved policies. Because basic human nature is to trust and help people, a seemingly innocent favor can put an organization at risk.

IDSs and physical protection measures ultimately require human intervention. Security guards can be at a fixed post or can patrol specific areas. Different organizations will have different needs from security guards. They may be required to check individual credentials and enforce filling out a sign-in log. They may be responsible for monitoring IDSs and expected to respond to alarms. They may need to issue and recover visitor badges, respond to fire alarms, enforce rules established by the company within the building, and control what materials can come into or go out of the environment. The guard may need to verify that doors, windows, safes, and vaults are secured; report identified safety hazards; enforce restrictions of sensitive areas; and escort individuals throughout facilities.

The security guard should have clear and decisive tasks that she is expected to fulfill. The guard should be fully trained on the activities she is expected to perform and on the responses expected from her in different situations. She should also have a central control point to check in to, two-way radios to ensure proper communication, and the necessary access into areas she is responsible for protecting.

929
The best security has a combination of security mechanisms and does not depend on
just one component of security. Thus, a security guard should be accompanied by other
surveillance and detection mechanisms.

Dogs
Dogs have proven to be highly useful in detecting intruders and other unwanted conditions. Their senses of smell and hearing outperform those of humans, and their intelligence and loyalty can be used for protection. The best security dogs go through intensive
training to respond to a wide range of commands and to perform many tasks. Dogs can be trained to hold an intruder at bay until security personnel arrive or to chase an
intruder and attack. Some dogs are trained to smell smoke so they can alert personnel
to a fire.
Of course, dogs cannot always know the difference between an authorized person and
an unauthorized person, so if an employee goes into work after hours, he can have more
on his hands than expected. Dogs can provide a good supplementary security mechanism.
EXAM TIP Because the use of guard dogs introduces significant risks to personal safety, which is paramount for CISSPs, exam answers that include dogs are likelier to be incorrect. Be on the lookout for these.

Auditing Physical Access
Physical access control systems can use software and auditing features to produce audit
trails or access logs pertaining to access attempts. The following information should be
logged and reviewed:

- The date and time of the access attempt
- The entry point at which access was attempted
- The user ID employed when access was attempted
- Any unsuccessful access attempts, especially if during unauthorized hours

Personnel Safety and Security
The single most valuable asset for an organization, and the one that involves the highest
moral and ethical standards, is its people. Our safety focus in security operations will
be on our own employees, but we also need to take proper steps to ensure the safety

As with audit logs produced by computers, access logs are useless unless someone actually reviews them. A security guard may be required to review these logs,

but a security
professional or a facility manager should also review these logs periodically. Management
needs to know where entry points into the facility exist and who attempts to use them.
Audit and access logs are detective controls, not preventive controls. They are used to
piece together a situation after the fact instead of attempting to prevent an access attempt
in the first place.

of visitors, clients, and anyone who enters into our physical or virtual spaces. While the
scope of safety is broader than information systems security, information
security professionals make important contributions to this effort.
EXAM TIP Human safety almost always trumps all other concerns. If an exam
question has a possible answer that focuses on safety, it is likelier to be the right one.

Travel
Personnel safety in the workplace is one thing, but how do we protect our staff while they
are traveling? There are a host of considerations we should take. The most basic one is to
determine the threat landscape at the destination. Some organizations go as far as having
country-specific briefings that are regularly updated and required for all staff traveling
overseas. This is obviously a resource-intensive proposition, but there are free alternatives
you can leverage. Many governments have departments or ministries that publish this
information for their citizens traveling abroad. For example, the U.S. Department of
State publishes travel advisories on its website for virtually any destination.
Speaking of these government entities, it is also important for traveling staff to know
the location and contact information for the nearest embassy or consulate. In case of
emergency, these offices provide a variety of important services. Depending on the threat
condition at the destination, it may be a good idea to notify these offices of staff members’
contact information, dates of travel, and places of lodging.
Hotel security starts by doing a bit of research ahead of the trip. If you’ve never stayed
in a specific hotel, a few minutes of web searching will give you a good indication of
whether or not it’s safe. Here are some other best practices that your organization’s staff
should consider when traveling:

• Ask for a room on the second floor. It reduces the risk of random criminal activity
and is still close enough to the ground to escape in case of an emergency even if
you can’t use the front door.
• Ask for and keep a hotel business card on your person at all times in case you have
to call the local police or embassy and provide your location in an emergency.
• Secure valuables in the in-room safe. It may not really be totally secure, but it
raises the bar on would-be thieves.
• Always use the security latch on the door when in the room.
• Keep your passport with you at all times when in a foreign country. Before the trip leave a photocopy of the passport with a trusted individual at home.

Security Training and Awareness
All these personal safety measures are good only if your organization’s staff actually knows
what they are and how and when to use them. Many organizations have mandatory training events for all staff, and personal security should be part of it. Keep in mind that

emergency procedures, panic codes/passwords, and travel security measures are quickly
forgotten if they are not periodically reinforced.

Emergency Management
A common tool for ensuring the safety of personnel during emergencies is the occupant
emergency plan (OEP). The OEP describes the actions that facility occupants should
take to ensure their safety during an emergency situation. This plan should address the
range of emergencies from individual to facility-wide, and it should be integrated into
the security operations of the organization.
Perhaps the best example of the intersection of safety and security occurs in the area
of physical access control. A well-designed system of physical access controls constrains
the movement of specific individuals in and out of certain spaces. For instance, we only
want authorized persons to enter the server room. But what if the server room offers the
best escape route for people who would normally not be allowed in it? While we would
not design a facility in which this would be the case, we sometimes end up occupying
less-than-ideal facilities. If this were the case, what process would we implement to ensure

we can get people out of the building quickly and not force them to take a circuitous
route that could put them in danger, but keeps them out of the sensitive area?
Another example involves access for emergency responders. If a fire alarm is triggered
in the building, how do we ensure we can evacuate all personnel while giving fire fighters
access to all spaces (without requiring them to break down doors)? In this context, how
do we simultaneously ensure the safety of our personnel while maintaining security of
our information systems?
Lastly, many modern physical access controls require electricity. If an electronic lock
does not have a battery backup, will it automatically unlock in the absence of power or
will it remain in the locked state? A fail-safe device is one that automatically moves to the
state that ensures safety in the event of a failure such as loss of power. Fail-safe controls,
while critical to human safety, must be carefully considered because they introduce risks
to the security of our information systems.

Duress

PART VII

Duress is the use of threats or violence against someone in order to force them to do
something they don’t want to do or otherwise wouldn’t do. Like any other threat, we
need to factor in duress in our risk assessment and figure out what (if anything) to do
about it. A popular example of a countermeasure for duress is the use of panic
buttons by bank tellers. The button is hidden where an assailant can’t see it but where the
teller can easily and discretely activate it to warn the police. A twist on this is the use
of duress codes in some alarm systems. The alarm has a keypad where an authorized
person can enter a secret code to deactivate it. The system can have two different codes:
a regular one that disarms the alarm, and a second one that also disarms the alarm
but also alerts authorities to an emergency. If someone was forcing you to disarm an
alarm, you’d enter the second code and they wouldn’t be able to know that you just
summoned the police.

Duress codes can also be verbal. For example, some alarm systems have an attendant call the facility to ensure everything is fine. If someone is under duress (and perhaps on speakerphone next to the assailant) you would want a discrete way for that person to convey that they are in danger. You could set up two possible responses, like "apple pie," which would mean you are in danger, and "sunshine," which would mean everything is truly fine. The key is to make the duress response sound completely benign.
Another situation to consider is when an assailant forces an employee to log into their account. You could set up a duress account with a username that is very similar to the real one. Upon login, the duress account looks just like the real one, except that it doesn't include sensitive content. The twist is that the duress password could do a range of things from activating full monitoring (like camera, keyboard, and packet logging) to quietly wiping the device in the background (useful for laptops being used away from the office).
Obviously, it would also generate an alert to security personnel that the user is in danger.

Chapter Review

This chapter was a bit of a whirlwind tour of many of the issues we need to manage as part of security operations. We covered a lot of ground, but keep in mind that these are all important topics you need to address in your organization if you want to operationalize security. Collectively, this chapter lays the foundation for the tasks many of us prefer to be doing: blocking bad actors from gaining access, finding the ones that sneak in, and frustrating their efforts to cause us harm. We dive into those in the next three chapters as we delve into day-to-day security operations, incident response, and dealing with disasters.

Quick Review

- SecOps (Security + Operations) is the integration of security and IT operations people, technology, and processes to reduce risks while improving business agility.
- Access to resources should be limited to authorized personnel, applications, and services and should be audited for compliance to stated policies.
- Least privilege means an individual should have just enough permissions and rights to fulfill his role in the company and no more.
- Need to know means we must first establish that an individual has a legitimate, job role–related need for a given resource before granting access to it.

• Separation of duties and responsibilities should be in place so that fraud cannot
take place without collusion of two or more people.
• Privileged account management formally enforces the principle of least privilege
on accounts with elevated rights.
• Job rotation means that, over time, more than one person fulfills the tasks of one
position within the organization, which provides backup and redundancy but also
helps identify fraudulent activities.

• A service level agreement (SLA) is a contract that states that a service provider
guarantees a certain level of service to a customer.
• Change management is the practice of minimizing the risks associated with the
addition, modification, or removal of anything that could have an effect on IT
services.
• Activities that involve change management include requesting, evaluating, planning,
implementing, reviewing, and closing or sustaining a change.
• Configuration management is the process of establishing and maintaining consistent
configurations on all our systems to meet organizational requirements.
• A baseline is the configuration of a system at a point in time as agreed upon by
the appropriate decision makers.
• Vulnerability management is the cyclical process of identifying vulnerabilities,
determining the risks they pose to the organization, and applying security
controls that bring those risks to acceptable levels.
• Patch management is the process for identifying, acquiring, installing, and verifying
patches for products and systems.
• Facilities that house systems that process sensitive information should have physical
access controls to limit access to authorized personnel only.
• Exterior fencing can be costly and unsightly, but can provide crowd control and
help control access to the facility, particularly if the fencing is eight feet or higher.
• Closed-circuit TV (CCTV) systems are made up of cameras, a controller and
digital video recording (DVR) system, and a monitor, but frequently also include
remote storage and remote client access.
• Locks are considered delaying devices to intruders.
• Some physical security controls may conflict with the safety of people. These
issues need to be addressed; human life is always more important than protecting
a facility or the assets it contains.
• Piggybacking occurs when an individual gains unauthorized access by using

someone else’s legitimate credentials or access rights, usually when the intruder
closely follows an authorized person through a door or gate.
• Proximity identification devices can be user activated (action needs to be taken
by a user) or system sensing (no action needs to be taken by the user).
• A transponder is a proximity-based access control reader that does not require action by the user. The reader transmits signals to the device, and the device responds with an access code.
• Intrusion detection devices include motion detectors, CCTVs, vibration sensors,
and electromechanical devices.
• Intrusion detection devices can be penetrated, are expensive to install and monitor, require human response, and are subject to false alarms.

• Security guards are expensive but provide flexibility in response to security breaches and can deter intruders from attempting an attack.
• Dogs are very effective at detecting and deterring intruders, but introduce significant risks to personal safety.
• Duress is the use of threats or violence against someone in order to force them to
do something they don’t want to do or otherwise wouldn’t do.

Questions
Please remember that these questions are formatted and asked in a certain way for a
reason. Keep in mind that the CISSP exam is asking questions at a conceptual level.
Questions may not always have the perfect answer, and the candidate is advised against
always looking for the perfect answer. Instead, the candidate should look for the best
answer in the list.
1. Why should employers make sure employees take their vacations?
A. They have a legal obligation.
B. It is part of due diligence.
C. It is a way for fraud to be uncovered.
D. To ensure employees do not get burned out.

2. Which of the following best describes separation of duties and job rotation?
A. Separation of duties ensures that more than one employee knows how to

perform the tasks of a position, and job rotation ensures that one person cannot perform a high-risk task alone.
B. Separation of duties ensures that one person cannot perform a high-risk task alone, and job rotation can uncover fraud and ensure that more than one person knows the tasks of a position.
C. They are the same thing, but with different titles.
D. They are administrative controls that enforce access control and protect the organization’s resources.
3. If a programmer is restricted from updating and modifying production code,

what is this an example of?
A. Rotation of duties
B. Due diligence
C. Separation of duties
D. Controlling input values

4. What is the difference between least privilege and need to know?
A. A user should have least privilege that restricts her need to know.
B. A user should have a security clearance to access resources, a need to know

about those resources, and least privilege to give her full control of all resources.
C. A user should have a need to know to access particular resources, and least privilege should be implemented to ensure she only accesses the resources she has a need to know.
D. They are two different terms for the same issue.
5. Which of the following would not require updated documentation?
A. An antivirus signature update
B. Reconfiguration of a server
C. A change in security policy
D. The installation of a patch to a production server
6. A company needs to implement a CCTV system that will monitor a large area outside the facility. Which of the following is the correct lens combination for this?
A. A wide-angle lens and a small lens opening
B. A wide-angle lens and a large lens opening
C. A wide-angle lens and a large lens opening with a small focal length
D. A wide-angle lens and a large lens opening with a large focal length
7. Which of the following is not a true statement about CCTV lenses?
A. Lenses that have a manual iris should be used in outside monitoring.
B. Zoom lenses carry out focus functionality automatically.
C. Depth of field increases as the size of the lens opening decreases.
D. Depth of field increases as the focal length of the lens decreases.
8. What is true about a transponder?
A. It is a card that can be read without sliding it through a card reader.
B. It is a biometric proximity device.
C. It is a card that a user swipes through a card reader to gain access to a facility.
D. It exchanges tokens with an authentication server.
9. When is a security guard the best choice for a physical access control mechanism?
A. When discriminating judgment is required
B. When intrusion detection is required
C. When the security budget is low
D. When access controls are in place

10. Which of the following is not a characteristic of an electrostatic intrusion detection system?
A. It creates an electrostatic field and monitors for a capacitance change.
B. It can be used as an intrusion detection system for large areas.
C. It produces a balance between the electric capacitance and inductance of an object.
D. It can detect if an intruder comes within a certain range of an object.
11. What is a common problem with vibration-detection devices used for perimeter security?
A. They can be defeated by emitting the right electrical signals in the protected area.
B. The power source is easily disabled.
C. They cause false alarms.
D. They interfere with computing devices.
12. Which of the following is not considered a delaying mechanism?
A. Locks
B. Defense-in-depth measures
C. Warning signs
D. Access controls
13. What are the two general types of proximity identification devices?
A. Biometric devices and access control devices
B. Swipe card devices and passive devices
C. Preset code devices and wireless devices
D. User-activated devices and system sensing devices
14. Which is not a drawback of an intrusion detection system?
A. It’s expensive to install.
B. It cannot be penetrated.
C. It requires human response.
D. It’s subject to false alarms.
15. What is a cipher lock?
A. A lock that uses cryptographic keys
B. A lock that uses a type of key that cannot be reproduced
C. A lock that uses a token and perimeter reader
D. A lock that uses a keypad

16. If a cipher lock has a door delay option, what does that mean?
A. After a door is open for a specific period, the alarm goes off.
B. It can only be opened during emergency situations.
C. It has a hostage alarm capability.
D. It has supervisory override capability.

Answers
1. C. Many times, employees who are carrying out fraudulent activities do not take the vacation they have earned because they do not want anyone to find out what they have been doing. Forcing an employee to take a vacation means that someone else has to do that person’s job and can possibly uncover any misdeeds.
2. B. Rotation of duties enables an organization to have more than one person trained in a position and can uncover fraudulent activities. Separation of duties is