patches
or upgrades are applied to existing software, or when other changes to the system take
place, there is a good chance the system may no longer be providing its necessary
minimum level of protection (its baseline). Security personnel must assess the systems as
changes take place and ensure that the baseline level of security is always being met. If a
technician installs a patch on a system and does not ensure the baseline is still being met,
there could be new vulnerabilities introduced into the system that will allow attackers
easy access to the network.

NOTE Baselines that are not technology oriented should be created and enforced within organizations as well. For example, a company can mandate that while in the facility all employees must have a badge with a picture ID in view at all times. It can also state that visitors must sign in at a front desk and
be escorted while in the facility. If these rules are followed, then this creates
a baseline of protection.

Guidelines
Guidelines are recommended actions and operational guides to users, IT staff, operations
staff, and others when a specific standard does not apply. They can also be used as a recommended way to achieve specific standards when those do apply. Guidelines can deal
with the methodologies of technology, personnel, or physical security. Life is full of gray
areas, and guidelines can be used as a reference during those times. Whereas standards
are specific mandatory rules, guidelines are general approaches that provide the necessary
flexibility for unforeseen circumstances.
A policy might state that access to confidential data must be audited. A supporting
guideline could further explain that audits should contain sufficient information to allow
for reconciliation with prior reviews. Supporting procedures would outline the necessary
steps to configure, implement, and maintain this type of auditing.

Procedures
Procedures are detailed step-by-step tasks that should be performed to achieve a certain
goal. The steps can apply to users, IT staff, operations staff, security members, and others
who may need to carry out specific tasks. Many organizations have written

procedures on
how to install operating systems, configure security mechanisms, implement access control lists, set up new user accounts, assign computer privileges, audit activities, destroy
material, report incidents, and much more.
Procedures are considered the lowest level in the documentation chain because they
are closest to the computers and users (compared to policies) and provide detailed steps
for configuration and installation issues.
Procedures spell out how the policy, standards, and guidelines will actually be implemented in an operating environment. If a policy states that all individuals who access
confidential information must be properly authenticated, the supporting procedures will
explain the steps for this to happen by defining the access criteria for authorization, how
access control mechanisms are implemented and configured, and how access activities
are audited. If a policy states that backups should be performed, then the procedures will
define the detailed steps necessary to perform the backup, the timelines of backups, the
storage of backup media, and so on. Procedures should be detailed enough to be both
understandable and useful to a diverse group of individuals.

Implementation
To tie these items together, let’s walk through an implementation example. A corporation’s security policy indicates that confidential information should be properly protected.

Personnel Security
Although society has evolved to be extremely dependent upon technology in the workplace, people are still the key ingredient to a successful company. But in security circles,
people are often the weakest link. Either accidentally through mistakes or lack of training, or intentionally through fraud and malicious intent, personnel cause more serious
and hard-to-detect security issues than hacker attacks, outside espionage, or equipment
failure. Although the future actions of individuals cannot be predicted, it is possible to
minimize the risks by implementing preventive measures. These include hiring the most
qualified individuals, performing background checks, using detailed job descriptions,
providing necessary training, enforcing strict access controls, and terminating individuals
in a way that protects all parties involved.

PART I

It states the issue in very broad and general terms. A supporting standard mandates
that all customer information held in databases must be encrypted with the Advanced
Encryption Standard (AES) algorithm while it is stored and that it cannot be transmitted over the Internet unless IPSec encryption technology is used. The standard indicates
what type of protection is required and provides another level of granularity and explanation. The supporting procedures explain exactly how to implement the AES and IPSec
technologies, and the guidelines cover how to handle cases when data is accidentally
corrupted or compromised during transmission. Once the software and devices are configured as outlined in the procedures, this is considered the baseline that must always be
maintained. All of these work together to provide a company with a security structure.
Unfortunately, security policies, standards, procedures, baselines, and guidelines often
are written because an auditor instructed a company to document these items, but then
they are placed on a file server and are not shared, explained, or used. To be useful, they
must be put into action. Employees aren’t going to follow the rules if they don’t know the
rules exist. Security policies and the items that support them not only must be developed
but must also be implemented and enforced.
To be effective, employees need to know about security issues within these documents;
therefore, the policies and their supporting counterparts need visibility. Awareness
training, manuals, presentations, newsletters, and screen banners can achieve this
visibility. It must be clear that the directives came from senior management and that
the full management staff supports these policies. Employees must understand what is
expected of them in their actions, behaviors, accountability, and performance.
Implementing security policies and the items that support them shows due care by the
company and its management staff. Informing employees of what is expected of them
and the consequences of noncompliance can come down to a liability issue. For example,
if a company fires an employee because he was downloading pornographic material to
the company’s computer, the employee may take the company to court and win if the
employee can prove he was not properly informed of what was considered acceptable

and unacceptable use of company property and what the consequences were. Security awareness training is covered later in this chapter, but personnel security is much broader than that.

Several items can be put into place to reduce the possibilities of fraud, sabotage, misuse of information, theft, and other security compromises. Separation of duties (SoD) makes sure that one individual cannot complete a critical task by herself. In the movies, when a submarine captain needs to launch a nuclear missile to blow up the enemy and save (or end) civilization as we know it, the launch usually requires two codes to be entered into the launching mechanism by two different senior crewmembers. This is an example of separation of duties, and it ensures that the captain cannot complete such an important and terrifying task all by himself.

Separation of duties is a security control that can reduce the potential for fraud. For example, an employee cannot complete a critical financial transaction by herself. She will need to have her supervisor's approval before the transaction can be completed. There is usually a third person involved who verifies that this procedure was followed.

In an organization that practices separation of duties, collusion must take place for fraud to be committed. Collusion means that at least two people are working together to cause some type of destruction or fraud. In our example, the employee and her supervisor must be participating in the fraudulent activity to make it happen. Even if this were to happen, the third person who reviewed the transaction would provide a way to detect this collusion early enough (hopefully) to stop the transaction.

Two variations of separation of duties are split knowledge and dual control. In both cases, two or more individuals are authorized and required to perform a duty or task.

In the case of split knowledge, no one person knows or has all the details to perform a task. For example, two managers might be required to open a bank vault, with each only knowing part of the combination. In the case of dual control, two individuals are again authorized to perform a task, but both must be available and active in their participation

to complete the task or mission. For example, two officers must perform an identical keyturn in a nuclear missile submarine, each out of reach of the other, to launch a missile.
The control here is that no one person has the capability of launching a missile, because
they cannot reach to turn both keys at the same time.
These are examples of what is generally known as an m of n control, which is a control
that requires a certain number of agents (m) out of a pool of authorized agents (n) to
complete an operation. This type of control can also be called quorum authentication,
because it requires the collaboration of a certain number of individuals (the quorum). In
the bank vault example, if there were five managers authorized to open the vault and two
were required to actually open it, this would be a 2 of 5 control, since m = 2 and n = 5.
You don’t want to make n too big because that increases the odds that two individuals
could secretly conspire to do something harmful. On the other hand, you would not
want m and n to have the same value, since the loss of any one individual would render
the vault unopenable!
Job rotation (rotation of assignments) is an administrative detective control that can be
put into place to uncover fraudulent activities. No one person should stay in one position
for a long time because they may end up having too much control over a segment of the
business. Such total control could result in fraud or the misuse of resources. Employees
should be moved into different roles with the idea that they may be able to detect
suspicious activity carried out by the previous employee filling that position. This type of
control is commonly implemented in financial institutions.

Candidate Screening and Hiring
The issues, policies, and procedures discussed in the previous section are important to consider in the daily operations of your organization’s staff, but let’s not get too far ahead of
ourselves. Personnel security starts way before a staff member shows up for work. Hiring the
right candidate for a position can have a significant impact on the organization’s security.
Depending on the position to be filled, human resources should perform a level of
candidate screening to ensure that the company hires the right individual for

the right
job. Each candidate’s skills should be tested and evaluated, and the caliber and character
of the individual should be examined. Joe might be the best programmer in the state,
but if someone looks into his past and finds out he served prison time because he hacked
into a bank, the hiring manager might not be so eager to bring Joe into the organization.
Human resources should contact candidates’ references, review their military records,
if applicable, verify their educational background, obtain their credit report, check
out their publicly viewable social media presence, and, if necessary, require proof of a
recently administered negative drug test. Many times, candidates are able to conceal
important personal behaviors, which is why hiring practices now include scenario
questions, personality tests, and observations of the individual, instead of just looking
at a person’s work history. When a person is hired, he is bringing his skills and whatever
other baggage he carries. A company can reduce its heartache pertaining to personnel by
first conducting useful and careful hiring practices.
The goal is to hire the “right person” and not just hire a person for “right now.”
Employees represent an investment on the part of the organization, and by taking the
time and hiring the right people for the jobs, the organization will be able to maximize
its investment and achieve a better return. Many organizations place a lot of value on
determining whether a candidate is a good “cultural” fit. This means that the person will
blend well into the culture that already exists in the company. People who fit in are more
likely to follow the existing norms, policies, and procedures.
A detailed background check can reveal some interesting information. Things like
unexplained gaps in employment history, the validity and actual status of professional
certifications, criminal records, driving records, job titles that have been misrepresented,
credit histories, unfriendly terminations, appearances on suspected terrorist watch lists,
and even real reasons for having left previous jobs can all be determined through the use

PART I

Employees in sensitive areas should be forced to take their vacations, which is known
as a mandatory vacation. While they are on vacation, other individuals fill their positions

and thus can usually detect any fraudulent errors or activities. Two of the many ways to
detect fraud or inappropriate activities would be the discovery of activity on someone’s
user account while they’re supposed to be away on vacation, or if a specific problem
stopped while someone was away and not active on the network. These anomalies are
worthy of investigation. Employees who carry out fraudulent activities commonly do
not take vacations because they do not want anyone to figure out what they are doing
behind the scenes. This is why they must periodically be required to be away from the
organization for a period of time, usually two weeks. Placing someone on administrative
leave during an investigation is also a form of mandatory vacation.

of background checks. This has real benefit to the employer and the organization because
it serves as the first line of defense for the organization against being attacked from
within. Any negative information found in these areas could be indicators of potential
problems that the candidate could create for the company at a later date if hired. Take the
credit report, for instance. On the surface, the candidate’s credit standing may seem to be
personal information that the organization doesn’t need to know about, but if the report
indicates the potential employee has a poor credit standing and a history of financial
problems, your organization certainly won’t want to place that person in charge of its
accounting, or even the petty cash.
Ultimately, the goal of performing background checks is to achieve several different
things for the organization at the same time:

• Mitigate risk
• Lower hiring and training costs and the turnover rate for employees
• Protect customers and employees from someone who could potentially conduct malicious and dishonest actions that could harm the organization, its employees, and its customers as well as the general public

In many cases, it is also harder to go back and conduct background checks after the individual has been hired and is working, because there will need to be a specific
cause or reason for conducting this kind of investigation. If any employee moves to a
position of greater security sensitivity or potential risk, a follow-up investigation should

be considered.
Possible background check criteria could include

- National identification number trace
- Criminal check
- Sexual offender registry check
- Employment verification
- Education verification
- Professional reference verification
- Immigration check
- Professional license/certification verification
- Credit report
- Drug screening

Employment Agreements and Policies
Congratulations! Your organization found the right candidate who passed its screening
with flying colors and accepted the offer of employment. Now what? Depending on the jurisdiction in which your organization is located, it may be legally required as an
employer to enter into a contract or other agreement with the candidate in order for the

Onboarding, Transfers, and Termination Processes
Onboarding is the process of turning a candidate into a trusted employee who is able to
perform all assigned duties. Having a structured and well-documented onboarding process not only will make the new employee feel valued and welcome but will also ensure
that your organization doesn’t forget any security tasks. Though the specific steps will
vary by organization, the following are some that are pretty universal:

- The new employee attends all required security awareness training.
- The new employee must read all security policies, be given an opportunity to have any questions about the policies answered, and sign a statement indicating they understand and will comply with the policies.
- The new employee is issued all appropriate identification badges, keys, and access
tokens pursuant to their assigned roles.
- The IT department creates all necessary accounts for the new employee, who signs
into the systems and sets their passwords (or changes any temporary passwords).

hiring action to be official. Whether or not this is a requirement for your organization,
it is almost always a good idea to put this employment agreement in writing and ensure

that it is signed by both parties. If you are a hiring manager, you should always follow the guidance provided by your human resources and legal teams, but it is useful to be aware of how this all works.

One of the key elements of an employment agreement is a reference to the policies that are applicable to employees in their new roles. Again, depending on where you are in the world, some policies (typically those dealing with safety and welfare) may be required to be included or referenced in the agreement. At a minimum, the employment agreement should include language pointing to the employee manual or other repository of policies for your organization. The point is that every new hire should sign an agreement stating that they are aware of the policies with which they must comply as a condition of employment. This becomes particularly helpful if there are any allegations of misconduct later on. For example, absent a signed employment agreement, if an employee deliberately (or even maliciously) accesses a computer or files that she shouldn't, she could claim she was never told it was wrong and get off the hook. According to the Federal Bureau of Investigation (FBI) manual on prosecuting computer crimes, "it is relatively easy to prove that a defendant had only limited authority to access a computer in cases where the defendant's access was limited by restrictions that were memorialized in writing, such as terms of service, a computer access policy, a website notice, or an employment agreement or similar contract."

Another important element of an employment agreement is the establishment of a probationary period. This is a period of time during which it is relatively easy to fire the new employee for misconduct or just failing to live up to expectations. Depending on the laws in your jurisdiction, it could be difficult to get rid of an employee even if it's obvious they are not working out. A probationary period could be helpful should you decide that your new hire is not as good as you thought.

Organizations should develop nondisclosure agreements (NDAs) and require them to be signed by new employees to protect the organization and its sensitive information. NDAs

typically specify what is considered sensitive information, how it should be protected, when it can be shared with others, and how long these obligations last after the employee (or the agreement) is terminated.

One of the most overlooked issues in personnel security is what happens when an employee's role within the organization changes. This could be a promotion (or demotion), assumption of new additional roles, loss of old roles, transfer to another business unit, or perhaps the result of a total restructuring of a business unit. Typically, what happens is that whatever old authorizations the employee had are never taken away, but new ones are added. Over time, employees who've been transferred or reassigned could accumulate a very extensive set of authorizations on information systems that they no longer need to access. IT and security staff need to be involved in transfers and role changes so that they can determine what policies apply and which permissions should be added, left in place, or removed. The goal is to ensure that every staff member has the permissions they need to do their jobs, and not a single one more.

Unfortunately, sometimes organizations have to terminate employees. Because terminations can happen for a variety of reasons, and terminated people have different reactions, companies should have a specific set of procedures to follow with every termination to ensure that their security posture isn't undermined in the process. For example:

- The employee must leave the facility immediately under the supervision of a manager or security guard.
- The employee must surrender any identification badges or keys, be asked to complete an exit interview, and return company supplies.
- That user's accounts and passwords must be disabled or changed immediately.

These actions may seem harsh when they actually take place, but too many companies have been hurt by vengeful employees who have retaliated against the companies after their positions were revoked for one reason or another. If an employee is disgruntled in any way or the termination is unfriendly, that employee's accounts must be disabled right away, and all passwords on all systems must be changed.

Practical Tips on Terminations

Without previous arrangement, an employee cannot be compelled to complete an exit interview, despite the huge value to the company of conducting such interviews.

Neither can an employee be compelled to return company property, as a practical matter, if he or she simply chooses not to. The best way to motivate departing

employees to comply is to ensure that any severance package they may be eligible for is contingent upon completion of these tasks, and that means having them agree
to such conditions up-front, as part of their employment agreement.

Vendors, Consultants, and Contractors

Compliance Policies
There are many forms of liability that may pertain to your organization. Your organization
may be subject to external regulations that require special attention and compliance from
a security standpoint. Examples are healthcare providers in the United States, who fall
under the Healthcare Insurance Portability and Accountability Act (HIPAA); companies
that handle payment card information, which must follow the Payment Card Industry
Data Security Standard (PCI DSS); and organizations that handle personal information of
citizens of the European Union, which fall under the General Data Protection Regulation
(GDPR). Many more examples exist, but the point is that if your organization is regulated,

Many companies today could not perform their business functions without the services
of an assortment of vendors, consultants, and contractors who have different levels of
access to the companies' facilities and information systems. From the janitorial staff who
have physical access to virtually any area of a facility to the outsourced software developers in a different country who could introduce (willingly or otherwise) vulnerabilities
(or even backdoors) to the companies' most sensitive systems, the risks associated with
vendors, consultants, and contractors can be significant if left unmitigated.
There are a number of approaches to dealing with third parties in your environment from
an information security standpoint. One approach is to enter into service agreements that
require contractors to use security controls that are at least as stringent as your organization's
security controls, and to prove it. The service agreement could include specific requirements
for security controls or leverage existing standards such as the International Organization
for Standardization (ISO) 27001 certification (which we discuss in Chapter 4).

Either way,
the agreement must specify a way to verify compliance with the contractual obligations and
clearly state the penalties for failing to meet those obligations.
Another approach to dealing with third parties is to assume that vendors, consultants,
and contractors are untrusted and place strict controls around every aspect of their
performance. For example, you could require that janitors be escorted by designated
employees and that outsourced developers work on virtual desktop infrastructure under
the control of your organization. You could also require that highly sensitive assets (e.g.,
proprietary algorithms, trade secrets, and customer data) be off limits to these third
parties. This approach will likely reduce certain risks but may not be ideal for building
partnerships or engendering mutual trust.
There is no single best way to deal with the security issues inherent in working with third
parties. As with every aspect of personnel security, you should work in close coordination
with your business units, human resources staff, and legal counsel. Coordinating with
legal counsel is particularly critical, because your organization’s liability may (and often
does) extend to the actions and inactions of your vendors, consultants, and contractors.
For example, if your organization’s network is breached because one of your contractors
violated policies and that breach resulted in customers’ PII being stolen and causing
them financial losses, your company could be liable for their damages. This is known as
downstream liability.

then your personnel security practices must comply with these regulations. As a security
leader, you should know which regulations apply to your organization and how security
policies, including personnel security ones, work to ensure regulatory compliance.

Privacy Policies
Even if your organization doesn’t fall under GDPR or any of the myriad of similar privacy regulations and laws, there are good reasons for you to ensure that your organization
has a privacy policy and that your information security practices are aligned with it. For
example, suppose you have a policy that allows employees to privately check

personal
webmail during their breaks, and you also have a policy of decrypting and inspecting
all web traffic on your networks to ensure no adversaries are using encryption to sneak
around your security controls. These two policies could be in conflict with each other.
Worse yet, an employee could sue for violation of privacy if his e-mail messages are intercepted and read by your security team.

Security Awareness, Education, and Training Programs

Even if you develop security policies that protect organizational assets and are aligned
with all relevant laws and regulations, it is all for naught if nobody knows what they
are expected to do. For an organization to achieve the desired results of its security
program, it must communicate the what, how, and why of security to its employees.
Security awareness training should be comprehensive, tailored for specific groups, and
organization-wide. It should repeat the most important messages in different formats;
be kept up to date; be entertaining, positive, and humorous; be simple to understand;
and—most important—be supported by senior management. Management must allocate
the resources for this activity and enforce its attendance within the organization.
The goal is for each employee to understand the importance of security to the company
as a whole and to each individual. Expected responsibilities and acceptable behaviors
must be clarified, and noncompliance repercussions, which could range from a warning
to dismissal, must be explained before being invoked. Security awareness training can
modify employees’ behavior and attitude toward security. This can best be achieved
through a formalized process of security awareness training.

Degree or Certification?

Some roles within the organization need hands-on experience and skill, meaning that
the hiring manager should be looking for specific industry certifications. Some positions
require more of a holistic and foundational understanding of concepts or a business
background, and in those cases a degree may be required. Table 1-3 provides more information on the differences between awareness, training, and education.

Training

Education

Attribute

“What”

“How”

“Why”

Level

Information

Knowledge

Insight

Learning
objective

Recognition and
retention

Skill

Understanding

Example
teaching
method

Media:
Videos
Newsletters
Posters
CBT
Social engineering
testing

Practical Instruction:
Lecture and/or demo
Case study
Hands-on practice

Theoretical Instruction:
Seminar and discussion
Reading and study
Research

Test
measure

True/False, multiple
choice (identify
learning)

Problem solving—i.e.,
recognition and resolution
(apply learning)

Essay (interpret learning)

Impact
timeframe

Short-term

Intermediate

Long-term

Table 1-3 Aspects of Awareness, Training, and Education

Methods and Techniques to Present Awareness and Training
Because security is a topic that can span many different aspects of an organization, it can be difficult to communicate the correct information to the right individuals. By using a formalized process for security awareness training, you can establish a method that will provide you with the best results for making sure security requirements are presented to the right people in an organization. This way you can make sure everyone understands what is outlined in the organization's security program, why it is important, and how it fits into the individual's role in the organization. The higher levels of training typically are more general and deal with broader concepts and goals, and as the training moves down to specific jobs and tasks, it becomes more situation specific as it directly applies to certain positions within the company.
A security awareness program is typically created for at least three types of audiences: management, staff, and technical employees. Each type of awareness training must be geared toward the individual audience to ensure each group understands its particular responsibilities, liabilities, and expectations. If technical security training were given to senior management, their eyes would glaze over as soon as protocols and firewalls were mentioned. On the flip side, if legal ramifications, company liability issues pertaining to

protecting data, and shareholders' expectations were discussed with the IT group, they would quickly turn to their smartphone and start tweeting, browsing the Internet, or texting their friends.

Members of senior management would benefit the most from a short, focused security awareness orientation that discusses corporate assets and financial gains and losses pertaining to security. They need to know how stock prices can be negatively affected by compromises, understand possible threats and their outcomes, and know why security

must be integrated into the environment the same way as other business processes.

Because members of management must lead the rest of the company in support of security, they must gain the right mindset about its importance.

Middle management would benefit from a more detailed explanation of the policies, procedures, standards, and guidelines and how they map to the individual departments for which each middle manager is responsible. Middle managers should be taught why their support for their specific departments is critical and what their level of responsibility is for ensuring that employees practice safe computing activities. They should also be shown how the consequences of noncompliance by individuals who report to them can affect the company as a whole and how they, as managers, may have to answer for such indiscretions.

Staff training, which typically involves the largest portion of an organization, should provide plenty of examples of specific behaviors that are expected, recommended, and forbidden. This is an opportunity to show how alert users can be sensors providing early warning of attacks, which can dramatically improve the security posture of any organization.

This can be accomplished by training the staff to recognize and report the sorts of attacks they are likely to face. Conversely, it is important to also show the consequences, organizational and personal, of being careless or violating policies and procedures.

The technical departments must receive a different presentation that aligns more to their

daily tasks. They should receive a more in-depth training to discuss technical configurations,
incident handling, and how to recognize different types of security compromises.
Perhaps no other topic is more important or better illustrates the need to communicate
security issues differently to each of these three audiences than the topic of social
engineering. Social engineering is the deliberate manipulation of a person or group of
persons to persuade them to do something they otherwise wouldn't or shouldn't. In a
security context, this typically means getting a member of the organization to violate
a security policy or procedure or to help an attacker compromise a system. The most
common form of social engineering is phishing, which is the use of e-mail messages
to perform social engineering. While all employees should know that they should not
click on links or open attachments in e-mail messages if they don't recognize the sender,
executives, managers, and end users should be presented the problem in a different light.
Regardless of how the training is presented, it is usually best to have each employee sign
a document indicating they have heard and understand all the security topics discussed
and that they also understand the ramifications of noncompliance. This reinforces the
policies' importance to the employee and also provides evidence down the road if the
employee claims they were never told of these expectations. Awareness training should
happen during the hiring process and at least annually after that. Attendance of training
should also be integrated into employment performance reports.
Various methods should be employed to reinforce the concepts of security awareness.
Things like screen banners, employee handbooks, and even posters can be used as ways
to remind employees about their duties and the necessities of good security practices.
But there are other ways to drive employee engagement. For example, gamification is
the application of elements of game play to other activities such as security awareness
training. By some accounts, gamification can improve employees' skill retention by
40 percent. Another approach is to leverage employees who are not formally part of the

Periodic Content Reviews

The only constant in life is change, so it should come as no surprise that after we develop the curricula and materials for security awareness training, we have to keep them up to date by conducting periodic content reviews. It is essential that this be a deliberate process and not done in an ad hoc manner. One way to do this is to schedule refreshes at specific intervals like semi-annually or yearly and assign the task to an individual owner. This person would work with a team to review and update the plan and materials but is ultimately responsible for keeping the training up to date.

Another approach is to have content reviews be triggered by other events. For example, reviews can be required whenever any of the following occur:

- A security policy is added, changed, or discontinued
- A major incident (or pattern of smaller incidents) occurs that could've been avoided or mitigated through better security awareness
- A major new threat is discovered
- A major change is made to the information systems or security architecture
- An assessment of the training program shows deficiencies

Program Effectiveness Evaluation

Many organizations treat security awareness training as a "check in the box" activity that is done simply to satisfy a requirement. The reality, however, is that effective training has both objectives (why we do it) and outcomes (what people can do after participating in it). The objectives are usually derived from senior-level policies or directives and drive the development of outcomes, which in turn drive the content and methods of delivery. For example, if the objective is reducing the incidence of successful phishing attacks, then it would be appropriate to pursue an outcome of having end users be able to detect a phishing e-mail. Both the objective and the outcome are measurable, which makes it easier to answer the question "is this working?"

We can evaluate whether the security training program is effective in improving an organization's security posture by simply measuring things before the training and then after it. Continuing the earlier example, we could keep track of the number of successful phishing attacks and see what happens to that number after the training has been conducted. This would be an assessment of the objective. We could also take trained and untrained users and test their ability to detect phishing e-mails. We would expect the trained users to

fare better at this task, which would test the outcome. If we see that the number of phishing

security program and yet have the skills and aptitudes that make them security advocates within their own business units. These individuals can be identified and deliberately nurtured to act as conduits between business units and the security program. They can become security champions, which are members of an organization that, though their job descriptions do not include security, inform and encourage the adoption of security practices within their own teams.

attacks remains unchanged (or worse, grows) or that the users are no better at detecting phishing e-mails after the training, then maybe the program is not effective. When assessing the effectiveness of a training program, it is very important to analyze the data and not jump to conclusions. In the phishing example, there are many possible explanations for the lack of improvement. Maybe the adversaries are sending moresophisticated messages that are harder to detect. Similarly, the results could simply show that the users just don’t care and will continue to click links and open attachments until the consequences become negative enough for them. The point is to consider the root causes of the measurements when assessing the training.

Professional Ethics

Security awareness and training, of course, build on the notion that there are right ways and wrong ways in which to behave. This is the crux of ethics, which can be based on many different issues and foundations. Ethics can be relative to different situations and interpreted differently from individual to individual. Therefore, they are often a topic of debate. However, some ethics are less controversial than others, and these types of ethics are easier to expect of all people.

An interesting relationship exists between law and ethics. Most often, laws are based on ethics and are put in place to ensure that others act in an ethical way. However, laws do not apply to everything—that is when ethics should kick in. Some things may not be

illegal, but that does not necessarily mean they are ethical.
Certain common ethical fallacies are used by many in the computing world to justify
unethical acts. They exist because people look at issues differently and interpret (or
misinterpret) rules and laws that have been put into place. The following are examples
of these ethical fallacies:

• Hackers only want to learn and improve their skills. Many of them are not making a profit off of their deeds; therefore, their activities should not be seen as illegal or unethical.
• The First Amendment protects and provides the right for U.S. citizens to write viruses.
• Information should be shared freely and openly; therefore, sharing confidential
information and trade secrets should be legal and ethical.
• Hacking does not actually hurt anyone.

(ISC)2 Code of Professional Ethics
(ISC)2 requires all certified system security professionals to commit to fully supporting
its Code of Ethics. If a CISSP intentionally or knowingly violates this Code of Ethics, he
or she may be subject to a peer review panel, which will decide whether the certification
should be revoked.
The (ISC)2 Code of Ethics for the CISSP is listed on the (ISC)2 site at https://www
.isc2.org/Ethics. The following list is an overview, but each CISSP candidate should read

• Protect society, the common good, necessary public trust and confidence, and the
infrastructure
• Act honorably, honestly, justly, responsibly, and legally
• Provide diligent and competent service to principals
• Advance and protect the profession

Organizational Code of Ethics
More regulations are requiring organizations to have an ethical statement and potentially
an ethical program in place. The ethical program is to serve as the “tone at the top,”
which means that the executives need to ensure not only that their employees are acting
ethically but also that they themselves are following their own rules. The main goal is to
ensure that the motto “succeed by any means necessary” is not the spoken or unspoken

culture of a work environment. Certain structures can be put into place that provide a
breeding ground for unethical behavior. If the CEO gets more in salary based on stock
prices, then she may find ways to artificially inflate stock prices, which can directly hurt
the investors and shareholders of the company. If managers can only be promoted based
on the amount of sales they bring in, these numbers may be fudged and not represent
reality. If an employee can only get a bonus if a low budget is maintained, he might be
willing to take shortcuts that could hurt company customer service or product
development. Although ethics seem like things that float around in the ether and make us feel
good to talk about, they have to be actually implemented in the real corporate world
through proper business processes and management styles.

The Computer Ethics Institute
The Computer Ethics Institute is a nonprofit organization that works to help advance
technology by ethical means.
The Computer Ethics Institute has developed its own Ten Commandments of
Computer Ethics:
1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people’s computer work.
3. Thou shalt not snoop around in other people’s computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.

the full version and understand the Code of Ethics before attempting this exam. The
code’s preamble makes it clear that “[t]he safety and welfare of society and the common
good, duty to our principals, and to each other, requires that we adhere, and be seen to
adhere, to the highest ethical standards of behavior.” It goes on to provide four canons
for CISSPs:

7. Thou shalt not use other people’s computer resources without authorization or
proper compensation.
8. Thou shalt not appropriate other people’s intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or
the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and

respect
for your fellow humans.

Chapter Review

This chapter laid out some of the fundamental principles of cybersecurity: the meaning of security, how it is governed, and the means by which it is implemented in an enterprise. It then focused on the most important aspect of security: people. They are the most important asset to any organization and can also be the greatest champions, or underminers, of cybersecurity. The difference lies in who we hire, what roles we assign to them, and how we train them. Bring the right people into the right seats and train them well and you'll have a robust security posture. Do otherwise at your own peril.

Our collective goal in information systems security boils down to ensuring the availability, integrity, and confidentiality of our information in an environment rich in influencers. These include organizational goals, assets, laws, regulations, privacy, threats, and, of course, people. Each of these was discussed in some detail in this chapter. Along the way, we also covered tangible ways in which we can link security to each of the influencers. As CISSPs we must be skilled in creating these linkages, as we are trusted to be able to apply the right solution to any security problem.

Quick Review

- The objectives of security are to provide confidentiality, integrity, availability, authenticity, and nonrepudiation.
- Confidentiality means keeping unauthorized entities (be they people or processes) from gaining access to information assets.
- Integrity means that that an asset is free from unauthorized alterations.
- Availability protection ensures reliability and timely access to data and resources to authorized individuals.
- Authenticity protections ensure we can trust that something comes from its claimed source.
- Nonrepudiation, which is closely related to authenticity, means that someone cannot disavow being the source of a given action.
- A vulnerability is a weakness in a system that allows a threat source to compromise its security.

- A threat is any potential danger that is associated with the exploitation of

a vulnerability.
• A threat source (or threat agent, or threat actor) is any entity that can exploit
a vulnerability.
• A risk is the likelihood of a threat source exploiting a vulnerability and the corresponding business impact.
• A control, or countermeasure, is put into place to mitigate (reduce) the potential risk.
• Security governance is a framework that provides oversight, accountability, and compliance.
• An information security management system (ISMS) is a collection of policies, procedures, baselines, and standards that an organization puts in place to make sure that its security efforts are aligned with business needs, streamlined, and effective and that no security controls are missing.
• An enterprise security architecture implements an information security strategy
and consists of layers of solutions, processes, and procedures and the way they are
linked across an enterprise strategically, tactically, and operationally.
• An enterprise security architecture should tie in strategic alignment, business
enablement, process enhancement, and security effectiveness.
• Security governance is a framework that supports the security goals of an organization being set and expressed by senior management, communicated throughout the different levels of the organization, and consistently applied and assessed.
• Senior management always carries the ultimate responsibility for the organization.
• A security policy is a statement by management dictating the role security plays
in the organization.
• Standards are documents that describe specific requirements that are compulsory
in nature and support the organization’s security policies.
• A baseline is a minimum level of security.
• Guidelines are recommendations and general approaches that provide advice and flexibility.
• Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal.
• Job rotation and mandatory vacations are administrative security controls that can help detect fraud.
• Separation of duties ensures no single person has total control over a critical
activity or task.
• Split knowledge and dual control are two variations of separation of duties.

• Social engineering is an attack carried out to manipulate a person into providing
sensitive data to an unauthorized individual.
• Security awareness training should be comprehensive, tailored for specific groups,

and organization-wide.
• Gamification is the application of elements of game play to other activities such
as security awareness training.
• Security champions, which are members of an organization that, though their job descriptions do not include security, inform and encourage the adoption of security practices within their own teams.
• Professional ethics codify the right ways for a group of people to behave.

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. Which factor is the most important item when it comes to ensuring security is successful in an organization?
A. Senior management support
B. Effective controls and implementation methods
C. Updated and relevant security policies and procedures
D. Security awareness by all employees

Use the following scenario to answer Questions 2–4. Todd is a new security manager and
has the responsibility of implementing personnel security controls within the financial
institution where he works. Todd knows that many employees do not fully understand
how their actions can put the institution at risk; thus, he needs to develop a security
awareness program. He has determined that the bank tellers need to get a supervisory
override when customers have checks over $3,500 that need to be cashed. He has also uncovered that some employees have stayed in their specific positions within the
company for over three years. Todd would like to be able to investigate some of the
activities of bank personnel to see if any fraudulent activities have taken place. Todd is
already ensuring that two people must use separate keys at the same time to open the
bank vault.

A. Separation of duties
B. Job rotation
C. Mandatory vacations

D. Split knowledge

3. If the financial institution wants to ensure that fraud cannot happen successfully
unless collusion occurs, what should Todd put into place?
A. Separation of duties
B. Job rotation
C. Social engineering
D. Split knowledge

4. Todd wants to be able to prevent fraud from taking place, but he knows that some
people may get around the types of controls he puts into place. In those situations
he wants to be able to identify when an employee is doing something suspicious.
Which of the following incorrectly describes what Todd is implementing in this scenario and what those specific controls provide?
A. Separation of duties, by ensuring that a supervisor must approve the cashing of

a check over $3,500. This is an administrative control that provides preventive protection for Todd's organization.
B. Job rotation, by ensuring that one employee only stays in one position for up to three months at a time. This is an administrative control that provides detective capabilities.
C. Security awareness training, which can also emphasize enforcement.
D. Dual control, which is an administrative detective control that can ensure that
two employees must carry out a task simultaneously.
5. Which term denotes a potential cause of an unwanted incident, which may result
in harm to a system or organization?
A. Vulnerability
B. Exploit
C. Threat
D. Attacker

PART I

2. Todd documents several fraud opportunities that the employees have at the financial institution so that management understands these risks and allocates the funds and resources for his suggested solutions. Which of the following best describes the control Todd should put into place to be able to carry out fraudulent investigation activity?

6. A CISSP candidate signs an ethics statement prior to taking the CISSP examination.
Which of the following would be a violation of the (ISC)2 Code of Ethics that could cause the candidate to lose his or her certification?
A. E-mailing information or comments about the exam to other CISSP candidates
B. Submitting comments on the questions of the exam to (ISC)2

C. Submitting comments to the board of directors regarding the test and content

of the class
D. Conducting a presentation about the CISSP certification and what the certification means
7. You want to ensure that your organization’s finance department, and only the finance department, has access to the organization’s bank statements. Which of the security properties would be most important?
A. Confidentiality
B. Integrity
C. Availability
D. Both A and C
8. You want to make use of the OpenOffice productivity software suite mandatory across your organization. In what type of document would you codify this?
A. Policy
B. Standard
C. Guideline
D. Procedure
9. For an enterprise security architecture to be successful in its development and
implementation, which of the following items is not essential?
A. Strategic alignment
B. Security guidelines
C. Business enablement
D. Process enhancement
10. Which of the following practices is likeliest to mitigate risks when considering
a candidate for hiring?
A. Security awareness training
B. Nondisclosure agreement (NDA)
C. Background checks
D. Organizational ethics

Answers
2. C. Mandatory vacation is an administrative detective control that allows for an
organization to investigate an employee’s daily business activities to uncover any
potential fraud that may be taking place. The employee should be forced to be away from the organization for a two-week period, and another person should be put into that role. The idea is that the person who was rotated into that position
may be able to detect suspicious activities.
3. A. Separation of duties is an administrative control that is put into place to ensure
that one person cannot carry out a critical task by himself. If a person were able to
carry out a critical task alone, this could put the organization at risk. Collusion is
when two or more people come together to carry out fraud. So if a task was split

between two people, they would have to carry out collusion (working together) to complete that one task and carry out fraud.
4. D. Dual control is an administrative preventive control. It ensures that two people must carry out a task at the same time, as in two people having separate keys when opening the vault. It is not a detective control. Notice that the question
asks what Todd is not doing. Remember that on the exam you need to choose the best answer. In many situations you will not like the question or the corresponding
answers on the CISSP exam, so prepare yourself. The questions can be tricky, which is one reason why the exam itself is so difficult.
5. C. The question provides the definition of a threat. The term attacker (option D)
could be used to describe a threat agent that is, in turn, a threat, but use of this
term is much more restrictive. The best answer is a threat.
6. A. A CISSP candidate and a CISSP holder should never discuss with others what was on the exam. This degrades the usefulness of the exam to be used as a tool to
test someone's true security knowledge. If this type of activity is uncovered, the
person could be stripped of their CISSP certification because this would violate the terms of the NDA into which the candidate enters prior to taking the test. Violating an NDA is a violation of the ethics canon that requires CISSPs to act honorably, honestly, justly, responsibly, and legally.
7. D. Confidentiality is ensuring that unauthorized parties (i.e., anyone other than
finance department employees) cannot access protected assets. Availability is ensuring that authorized entities (i.e., finance) maintain access to assets. In this
case, both confidentiality and availability are important to satisfy the requirements
as stated.
8. B. Standards describe mandatory activities, actions, or rules. A policy is intended
to be strategic, so it would not be the right document. A procedure describes the
manner in which something must be done, which is much broader than is needed to make using a particular software suite mandatory across your organization. Finally, guidelines are recommended but optional practices.

PART I

1. A. Without senior management's support, a security program will not receive the
necessary attention, funds, resources, and enforcement capabilities.

9. B. Security guidelines are optional recommendations on issues that are not covered
by mandatory policies, standards, or procedures. A successful enterprise security

architecture is aligned with the organization’s strategy, enables its business, and
enhances (rather than hinders) its business processes.
10. C. The best way to reduce risk is to conduct background checks before you offer
employment to a candidate. This ensures you are hiring someone whose past has
been examined for any obviously disqualifying (or problematic) issues. The next
step would be to sign an employment agreement that would include an NDA,
followed by onboarding, which would include security awareness training and
indoctrination into the organizational code of ethics.

↟CHAPTER

Risk Management
This chapter presents the following:
• Risk management (assessing risks, responding to risks, monitoring risks)
• Supply chain risk management
• Business continuity

A ship in harbor is safe, but that is not what ships are built for.
—William G.T. Shedd

We next turn our attention to the concept that should underlie every decision made
when defending our information systems: risk. Risk is so important to understand as a
cybersecurity professional that we not only cover it in detail in this chapter (one of the
longest in the book) but also return to it time and again in the rest of the book. We start
off narrowly by focusing on the vulnerabilities in our organizations and the threats that
would exploit them to cause us harm. That sets the stage for an in-depth discussion of
the main components of risk management: framing, assessing, responding to, and
monitoring risks. We pay particular attention to supply chain risks, since these represent a big
problem to which many organizations pay little or no attention. Finally, we’ll talk about
business continuity because it is so closely linked to risk management. We’ll talk about
disaster recovery, a closely related concept, in later chapters.

Risk Management Concepts
Risk in the context of security is the likelihood of a threat source exploiting
a vulnerability and the corresponding business impact. Risk management (RM) is the process of
identifying and assessing risk, reducing it to an acceptable level, and ensuring it remains
at that level. There is no such thing as a 100-percent-secure environment. Every
environment has vulnerabilities and threats. The skill is in identifying these threats, assessing the
probability of them actually occurring and the damage they could cause, and then taking

the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.
Risks to an organization come in different forms, and they are not all computer related. As we saw in Chapter 1, when a company acquires another company, it takes
on a lot of risk in the hope that this move will increase its market base, productivity,

and profitability. If a company increases its product line, this can add overhead, increase
the need for personnel and storage facilities, require more funding for different materials,
and maybe increase insurance premiums and the expense of marketing campaigns. The
risk is that this added overhead might not be matched in sales; thus, profitability will be
reduced or not accomplished.
When we look at information security, note that an organization needs to be aware of
several types of risk and address them properly. The following items touch on the major
categories:

• Physical damage Fire, water, vandalism, power loss, and natural disasters
• Human interaction Accidental or intentional action or inaction that can disrupt productivity
• Equipment malfunction Failure of systems and peripheral devices
• Inside and outside attacks Hacking, cracking, and attacking
• Misuse of data Sharing trade secrets, fraud, espionage, and theft
• Loss of data Intentional or unintentional loss of information to unauthorized parties
• Application error Computation errors, input errors, and software defects
Threats must be identified, classified by category, and evaluated to calculate their
damage potential to the organization. Real risk is hard to measure, but prioritizing the
potential risks in the order of which ones must be addressed first is obtainable.

Holistic Risk Management

Who really understands risk management? Unfortunately, the answer to this question
is that not enough people inside or outside of the security profession really get it. Even
though information security is big business today, the focus all too often is on
applications, devices, viruses, and hacking. Although these items all must be considered and

weighed in risk management processes, they should be considered pieces of the overall
security puzzle, not the main focus of risk management.
Security is a business issue, but businesses operate to make money, not just to be
secure. A business is concerned with security only if potential risks threaten its bottom
line, which they can in many ways, such as through the loss of reputation and customer
base after a database of credit card numbers is compromised; through the loss of
thousands of dollars in operational expenses from a new computer worm; through the
loss of proprietary information as a result of successful company espionage attempts;
through the loss of confidential information from a successful social engineering attack;
and so on. It is critical that security professionals understand these individual threats, but
it is more important that they understand how to calculate the risk of these threats and
map them to business drivers.

• Organization view (Tier 1) Concerned with risk to the organization as a whole, which means it frames the rest of the conversation and sets important parameters such as the risk tolerance level.
• Mission/business process view (Tier 2) Deals with the risk to the major functions of the organization, such as defining the criticality of the information
flows between the organization and its partners or customers.
• Information systems view (Tier 3) Addresses risk from an information systems perspective. Though this is where we will focus our discussion, it is important to
understand that it exists within the context of (and must be consistent with) other,
more encompassing risk management efforts.

These tiers are dependent on each other, as shown in Figure 2-1. Risk management starts with decisions made at the organization tier, which flow down to the other two
tiers. Feedback on the effects of these decisions flows back up the hierarchy to inform
the next set of decisions to be made. Carrying out risk management properly means
that you have a holistic understanding of your organization, the threats it faces, the
countermeasures that can be put into place to deal with those threats, and continuous
monitoring to ensure the acceptable risk level is being met on an ongoing basis.

Figure 2-1 The three tiers of risk management (Source: NIST SP 800-39)

PART I

To properly manage risk within an organization, you have to look at it holistically.
Risk, after all, exists within a context. The U.S. National Institute of Standards and
Technology (NIST) Special Publication (SP) 800-39, Managing Information Security Risk, defines three tiers to risk management:

Information Systems Risk Management Policy
Proper risk management requires a strong commitment from senior leaders, a documented process that supports the organization's mission, an information systems risk
management (ISRM) policy, and a delegated ISRM team. The ISRM policy should be a subset of the organization's overall risk management policy (risks to an organization
include more than just information security issues) and should be mapped to the organizational security policies. The ISRM policy should address the following items:

• The objectives of the ISRM team
• The level of risk the organization will accept and what is considered an acceptable
level of risk
• Formal processes of risk identification
• The connection between the ISRM policy and the organization's strategic planning
processes
• Responsibilities that fall under ISRM and the roles to fulfill them
• The mapping of risk to internal controls
• The approach toward changing staff behaviors and resource allocation in response
to risk analysis
• The mapping of risks to performance targets and budgets
• Key metrics and performance indicators to monitor the effectiveness of controls
The ISRM policy provides the foundation and direction for the organization's security
risk management processes and procedures and should address all issues of information
security. It should provide direction on how the ISRM team communicates information on
the organization's risks to senior management and how to properly execute management's
decisions on risk mitigation tasks.

The Risk Management Team
Each organization is different in its size, security posture, threat profile, and security
budget. One organization may have one individual responsible for ISRM or a team

that
works in a coordinated manner. The overall goal of the team is to ensure that the organization is protected in the most cost-effective manner. This goal can be accomplished only
if the following components are in place:

• An established risk acceptance level provided by senior management
• Documented risk assessment processes and procedures
• Procedures for identifying and mitigating risks
• Appropriate resource and fund allocation from senior management
• Security awareness training for all staff members associated with information assets
• The ability to establish improvement (or risk mitigation) teams in specific areas
when necessary

Obviously, this list is a lot more than just buying a new shiny firewall and calling the
organization safe.
The ISRM team, in most cases, is not made up of employees with the dedicated task of risk management. It consists of people who already have a full-time job in the
organization and are now tasked with something else. Thus, senior management support
is necessary so proper resource allocation can take place.
Of course, all teams need a leader, and ISRM is no different. One individual should be
singled out to run this rodeo and, in larger organizations, this person should be spending
50 to 70 percent of their time in this role. Management must dedicate funds to making
sure this person receives the necessary training and risk analysis tools to ensure it is a
successful endeavor.

The Risk Management Process

By now you should believe that risk management is critical to the long-term security
(and even success) of your organization. But how do you get this done? NIST SP 800-39
describes four interrelated components that comprise the risk management process. These
are shown in Figure 2-2. Let’s consider each of these components briefly now, since they
will nicely frame the remainder of our discussion of risk management.

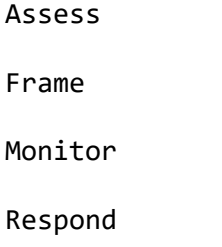
• Frame risk Risk framing defines the context within which all other risk activities take place. What are our assumptions and constraints? What are the organizational priorities? What is the risk tolerance of senior management?
• Assess risk Before we can take any action to mitigate risk, we have to assess

it. This is perhaps the most critical aspect of the process, and one that we will
discuss at length. If your risk assessment is spot-on, then the rest of the process
becomes pretty straightforward.
• Respond to risk By now, we've done our homework. We know what we should, must, and can't do (from the framing component), and we know what we're up against in terms of threats, vulnerabilities, and attacks (from the assess component).
Responding to the risk becomes a matter of matching our limited resources with our prioritized set of controls. Not only are we mitigating significant risk, but,
more importantly, we can tell our bosses what risk we can't do anything about because we're out of resources.

PART I

• The mapping of legal and regulation compliancy requirements to control and implement requirements
• The development of metrics and performance indicators so as to measure and manage various types of risks
• The ability to identify and assess new risks as the environment and organization
change
• The integration of ISRM and the organization's change control process to ensure
that changes do not introduce new vulnerabilities

Figure 2-2
The components
of the risk
management
process



• Monitor risk No matter how diligent we've been so far, we probably missed something. If not, then the environment likely changed (perhaps a new threat source emerged or a new system brought new vulnerabilities). In order to stay one step ahead of the bad guys, we need to continuously monitor the effectiveness of our controls against the risks for which we designed them.
You will notice that our discussion of risk so far has dealt heavily with the whole
framing process. In the preceding sections, we've talked about the organization (top to

bottom), the policies, and the team. The next step is to assess the risk, and what better
way to start than by understanding threats and the vulnerabilities they might exploit.

Overview of Vulnerabilities and Threats

To focus our efforts on the likely (and push aside the less likely) risks to our organizations, we need to consider what it is that we have that someone (or something) else may
be able to take, degrade, disrupt, or destroy. As we will see later (in the section “Assessing
Risks”), inventorying and categorizing our information systems is a critical early step
in the process. For the purpose of modeling the threat, we are particularly interested in
the vulnerabilities inherent in our systems that could lead to the compromise of their
confidentiality, integrity, or availability. We then ask the question, “Who would want to
exploit this vulnerability, and why?” This leads us to a deliberate study of our potential
adversaries, their motivations, and their capabilities. Finally, we determine whether a
given threat source has the means to exploit one or more vulnerabilities in order to attack
our assets.

NOTE We will discuss threat modeling in detail in Chapter 9.

Vulnerabilities

Information In almost every case, the information at the core of our information systems is the most valuable asset to a potential adversary. Information within a computer
information system (CIS) is represented as data. This information may be stored (data
at rest), transported between parts of our system (data in transit), or actively being used
by the system (data in use). In each of its three states, the information exhibits different
vulnerabilities, as listed in the following examples:

- Data at rest Data is copied to a thumb drive and given to unauthorized parties by an insider, thus compromising its confidentiality.
- Data in transit Data is modified by an external actor intercepting it on the network and then relaying the altered version (known as a man-in-the-middle or MitM attack), thus compromising its integrity.
- Data in use Data is deleted by a malicious process exploiting a “time-of-check to time-of-use” (TOC/TOU) or “race condition” vulnerability, thus compromising its availability.

Processes Most organizations implement standardized processes to ensure the consistency and efficiency of their services and products. It turns out,

however, that
efficiency is pretty easy to hack. Consider the case of shipping containers. Someone
wants to ship something from point A to point B, say a container of bananas from
Brazil to Belgium. Once the shipping order is placed and the destination entered, that
information flows from the farm to a truck carrier, to the seaport of origin to the ocean
carrier, to the destination seaport, to another truck carrier, and finally to its destination
at some distribution center in Antwerp. In most cases, nobody pays a lot of attention
to the address once it is entered. But what if an attacker knew this and changed the
address while the shipment was at sea? The attacker could have the shipment show up
at a different destination and even control the arrival time. This technique has actually
been used by drug and weapons smuggling gangs to get their “bananas” to where they
need them.
This sort of attack is known as business process compromise (BPC) and is commonly
targeted at the financial sector, where transaction amounts, deposit accounts, or other
parameters are changed to funnel money to the attackers’ pockets. Since business processes
are almost always instantiated in software as part of a CIS, process vulnerabilities can be
thought of as a specific kind of software vulnerability. As security professionals, however,

PART I

Everything built by humans is vulnerable to something. Our information systems, in
particular, are riddled with vulnerabilities even in the best-defended cases. One need only
read news accounts of the compromise of the highly protected and classified systems of
defense contractors and even governments to see that this universal principle is true. To
properly analyze vulnerabilities, it is useful to recall that information systems consist of
information, processes, and people that are typically, but not always, interacting with
computer systems. Since we discuss computer system vulnerabilities in detail in Chapter 6,
we will briefly discuss the other three components here.

it is important that we take a broader view of the issue and think about the

business
processes that are implemented in our software systems.
People Many security experts consider humans to be the weakest link in the security
chain. Whether or not you agree with this, it is important to consider the specific
vulnerabilities that people present in a system. Though there are many ways to exploit the
human in the loop, there are three that correspond to the bulk of the attacks, summarized
briefly here:

• Social engineering This is the process of getting a person to violate a security
procedure or policy, and usually involves human interaction or e-mail/text messages.
• Social networks The prevalence of social network use provides potential
attackers with a wealth of information that can be leveraged directly (e.g.,
blackmail) or indirectly (e.g., crafting an e-mail with a link that is likely to be
clicked) to exploit people.
• Passwords Weak passwords can be cracked in milliseconds using rainbow
tables and are very susceptible to dictionary or brute-force attacks. Even strong
passwords are vulnerable if they are reused across sites and systems.

Threats
As you identify the vulnerabilities that are inherent to your organization and its systems,
it is important to also identify the sources that could attack them. The International
Organization for Standardization and the International Electrotechnical Commission in
their joint ISO/IEC standard 27000 define a threat as a “potential cause of an unwanted
incident, which can result in harm to a system or organization.” While this may sound
somewhat vague, it is important to include the full breadth of possibilities. When a threat
is one or more humans, we typically use the term threat actor or threat agent. Let’s start
with the most obvious: malicious humans.
Cybercriminals Cybercriminals are the most common threat actors encountered by
individuals and organizations. Most cybercriminals are motivated by greed, but some
just enjoy breaking things. Their skills run the gamut, from so-called script kiddies with
just a basic grasp of hacking (but access to someone else’s scripts or tools) to sophisticated
cybercrime gangs who develop and sometimes sell or rent their services and tools to
others. Cybercrime is the fastest-growing sector of criminal activity in many countries.
One of the factors that makes cybercrime so pervasive is that every connected

device
is a target. Some devices are immediately monetizable, such as your personal smartphone
or home computer containing credentials, payment card information, and access to your
financial institutions. Other targets provide bigger payouts, such as the finance systems
in your place of work. Even devices that are not, by themselves, easily monetizable can
be hijacked and joined into a botnet to spread malware, conduct distributed
denial-ofservice (DDoS) attacks, or serve as staging bases from which to attack other targets.
Nation-State Actors Whereas cybercriminals tend to cast a wide net in an effort to
maximize their profits, nation-state actors (or simply state actors) are very selective in

Hacktivists Hacktivists use cyberattacks to effect political or social change. The term
covers a diverse ecosystem, encompassing individuals and groups of various skillsets
and capabilities. Hacktivists' preferred objectives are highly visible to the public or
yield information that, when made public, aims to embarrass government entities or
undermine public trust in them.
Internal Actors Internal actors are people within the organization, such as employees,
former employees, contractors, or business associates, who have inside information
concerning the organization's security practices, data, and computer systems. Broadly
speaking, there are two types of insider threats: negligent and malicious. A negligent insider
is one who fails to exercise due care, which puts their organization at risk. Sometimes,
these individuals knowingly violate policies or disregard procedures, but they are not doing
so out of malicious intent. For example, an employee could disregard a policy requiring
visitors to be escorted at all times because someone shows up wearing the uniform of a
telecommunications company and claiming to be on site to fix an outage. This insider trusts
the visitor, which puts the organization at risk, particularly if that person is an impostor.
The second type of insider threat is characterized by malicious intent. Malicious
insiders use the knowledge they have about their organization either for their own

advantage (e.g., to commit fraud) or to directly cause harm (e.g., by deleting sensitive files). While some malicious insiders plan their criminal activity while they are employees in good standing, others are triggered by impending termination actions. Knowing (or suspecting) that they're about to be fired, they may attempt to steal sensitive data (such as customer contacts or design documents) before their access is revoked. Other malicious insiders may be angry and plant malware or destroy assets in an act of revenge. This insider threat highlights the need for the "zero trust" secure design principle (discussed in Chapter 9). It is also a really good reason to practice the termination processes discussed in Chapter 1.

who they target. They use advanced capabilities to compromise systems and establish a persistent presence to allow them to collect intelligence (e.g., sensitive data, intellectual property, etc.) for extended periods. After their presence is established, state actors may use prepositioned assets to trigger devastating effects in response to world events. Though their main motivations tend to be espionage and gaining persistent access to critical infrastructure, some state actors maintain good relations with cybercrime groups in their own country, mostly for the purposes of plausible deniability. By collaborating with these criminals, state actors can make it look as if an attack against another nation was a crime and not an act of war. At least one country is known to use its national offensive cyber capabilities for financial profit, stealing millions of dollars all over the world.

Many security professionals consider state actors a threat mostly to government organizations, critical infrastructure like power plants, and anyone with sophisticated research and development capabilities. In reality, however, these actors can and do target other organizations, typically to use them as a springboard into their ultimate targets. So, even if you work for a small company that seems uninteresting to a foreign nation, you could find your company in a state actor's crosshairs.

In the wake of the massive leak of classified data attributed to Edward Snowden in
2012, there’s been increased emphasis on techniques and procedures for identifying and
mitigating the insider threat source. While the deliberate insider dominates the news, it is
important to note that the accidental insider can be just as dangerous, particularly if they
fall into one of the vulnerability classes described in the preceding section.
Nature Finally, the nonhuman threat source can be just as important as the ones we’ve previously discussed. Hurricane Katrina in 2005 and the Tohoku earthquake and
tsunami in 2011 serve as reminders that natural events can be more destructive than any
human attack. They also force the information systems security professional to consider
threats that fall way outside the norm. Though it is easier and, in many cases, cheaper to
address likelier natural events such as a water main break or a fire in a facility, one should
always look for opportunities to leverage countermeasures that protect against both mild
and extreme events for small price differentials.

Identifying Threats and Vulnerabilities
Earlier, it was stated that the definition of a risk is the probability of a threat exploiting a
vulnerability to cause harm to an asset and the resulting business impact. Many types of
threat actors can take advantage of several types of vulnerabilities, resulting in a variety
of specific threats, as outlined in Table 2-1, which represents only a sampling of the risks
many organizations should address in their risk management programs.
Other types of threats can arise in an environment that are much harder to identify
than those listed in Table 2-1. These other threats have to do with application and user
errors. If an application uses several complex equations to produce results, the threat can
be difficult to discover and isolate if these equations are incorrect or if the application is
using inputted data incorrectly. This can result in illogical processing and cascading errors
as invalid results are passed on to another process. These types of problems can lie within
application code and are very hard to identify.
Threat Actor

Can Exploit This Vulnerability

To Cause This Effect

Cybercriminal

Lack of antimalware software

Ransomed data

Nation-state actor

Password reuse in privileged accounts

Unauthorized access to confidential information

Negligent user

Misconfigured parameter in the operating system

Loss of availability due to a system malfunction

Fire

Lack of fire extinguishers

Facility and computer loss or damage, and possibly loss of life

Malicious insider

Poor termination procedures

Deletion of business-critical information

Hacktivist

Poorly written web application

Website defacement

Burglar

Lack of security guard

Breaking windows and stealing computers and devices

Table 2-1 Relationship of Threats and Vulnerabilities

Assessing Risks

A risk assessment, which is really a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls. After parts of a risk assessment are carried out, the results are analyzed. Risk analysis is a detailed examination of the components of risk that is used to ensure that security is cost-effective, relevant, timely, and responsive to threats. It is easy to apply too much security, not enough security, or the wrong security controls and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps organizations prioritize their risks and shows management the amount of resources that should be applied to protecting against those risks in a sensible manner.

EXAM TIP The terms risk assessment and risk analysis, depending on who you ask, can mean the same thing, or one must follow the other, or one is a subpart of the other. Here, we treat risk assessment as the broader effort, which is reinforced by specific risk analysis tasks as needed. This is how you should think of it for the CISSP exam.

User errors, whether intentional or accidental, are easier to identify by monitoring and auditing users' activities. Audits and reviews must be conducted to discover if employees are inputting values incorrectly into programs, misusing technology, or modifying data in an inappropriate manner.

After the ISRM team has identified the vulnerabilities and associated threats, it must investigate the ramifications of any of those vulnerabilities being exploited. Risks have loss potential, meaning that the organization could lose assets or revenues if a threat agent actually exploited a vulnerability. The loss may be corrupted data, destruction of systems and/or the facility, unauthorized disclosure of confidential information, a reduction in employee productivity, and so on. When performing a risk assessment, the team also must look at delayed loss when assessing the damages that can occur. Delayed loss is secondary in nature and takes place well after a vulnerability is exploited. Delayed loss may include damage to the organization's reputation, loss of market share, accrued late penalties, civil suits, the delayed collection of funds from customers, resources required to reimage other compromised systems, and so forth.

For example, if a company's web servers are attacked and taken offline, the immediate damage (loss potential) could be data corruption, the man-hours necessary to place the servers back online, and the replacement of any code or components required. The company could lose revenue if it usually accepts orders and payments via its website. If getting the web servers fixed and back online takes a full day, the company could lose a lot more sales and profits. If getting the web servers fixed and back online takes a full week, the company could lose enough sales and profits to not be able to pay other bills and expenses. This would be a delayed loss. If the company's customers lose confidence in it because of this activity, the company could lose business for months or years. This is a more extreme case of delayed loss.

These types of issues make the process of properly quantifying losses that specific threats could cause more complex, but they must be taken into consideration to ensure reality is represented in this type of analysis.

Risk analysis has four main goals:

- Identify assets and their value to the organization.
- Determine the likelihood that a threat exploits a vulnerability.
- Determine the business impact of these potential threats.
- Provide an economic balance between the impact of the threat and the cost of the countermeasure.

Risk analysis provides a cost/benefit comparison, which compares the annualized cost of controls to the potential cost of loss. A control, in most cases, should not be implemented unless the annualized cost of loss exceeds the annualized cost of the control itself. This means that if a facility is worth $100,000, it does not make sense to spend $150,000 trying to protect it.

It is important to figure out what you are supposed to be doing before you dig right in and start working. Anyone who has worked on a project without a properly defined scope can attest to the truth of this statement. Before an assessment is started, the team must carry out project sizing to understand what assets and threats should be evaluated. Most assessments are focused on physical security, technology security, or personnel

security.
Trying to assess all of them at the same time can be quite an undertaking.
One of the risk assessment team's tasks is to create a report that details the asset
valuations. Senior management should review and accept the list and use these values
to determine the scope of the risk management project. If management determines
at this early stage that some assets are not important, the risk assessment team should
not spend additional time or resources evaluating those assets. During discussions with
management, everyone involved must have a firm understanding of the value of the
security CIA triad—confidentiality, integrity, and availability—and how it directly
relates to business needs.
Management should outline the scope of the assessment, which most likely will be
dictated by organizational compliance requirements as well as budgetary constraints.
Many projects have run out of funds, and consequently stopped, because proper project
sizing was not conducted at the onset of the project. Don't let this happen to you.
A risk assessment helps integrate the security program objectives with the organization's
business objectives and requirements. The more the business and security objectives are
in alignment, the more successful both will be. The assessment also helps the organization
draft a proper budget for a security program and its constituent security components.
Once an organization knows how much its assets are worth and the possible threats those
assets are exposed to, it can make intelligent decisions about how much money to spend
protecting those assets.
A risk assessment must be supported and directed by senior management if it is to be
successful. Management must define the purpose and scope of the effort, appoint a team
to carry out the assessment, and allocate the necessary time and funds to conduct it. It is
essential for senior management to review the outcome of the risk assessment and to act
on its findings. After all, what good is it to go through all the trouble of a risk assessment
and not react to its findings? Unfortunately, this does happen all too often.

Asset Valuation

- Cost to acquire or develop the asset

• Cost to maintain and protect the asset
• Value of the asset to owners and users
• Value of the asset to adversaries
• Price others are willing to pay for the asset
• Cost to replace the asset if lost
• Operational and production activities affected if the asset is unavailable
• Liability issues if the asset is compromised
• Usefulness and role of the asset in the organization
• Impact of the asset's loss on the organization's brand or reputation

Understanding the value of an asset is the first step to understanding what security mechanisms should be put in place and what funds should go toward protecting it. A very important question is how much it could cost the organization to not protect the asset.

PART I

To understand possible losses and how much we may want to invest in preventing them, we must understand the value of an asset that could be impacted by a threat. The value placed on information is relative to the parties involved, what work was required to develop it, how much it costs to maintain, what damage would result if it were lost or destroyed, how much money enemies would pay for it, and what liability penalties could be endured. If an organization does not know the value of the information and the other assets it is trying to protect, it does not know how much money and time it should spend on protecting them. If the calculated value of your company's secret formula is x, then the total cost of protecting it should be some value less than x. Knowing the value of our information allows us to make quantitative cost/benefit comparisons as we manage our risks.

The preceding logic applies not only to assessing the value of information and protecting it but also to assessing the value of the organization's other assets, such as facilities, systems, and even intangibles like the value of the brand, and protecting them. The value of the organization's facilities must be assessed, along with all printers, workstations, servers, peripheral devices, supplies, and employees. You do not know how much is in danger of being lost if you don't know what you have and what it is worth in the first place.

The actual value of an asset is determined by the importance it has to the organization as a whole. The value of an asset should reflect all identifiable costs that would arise if the asset were actually impaired. If a server cost $4,000 to purchase, this

value should
not be input as the value of the asset in a risk assessment. Rather, the cost of replacing or
repairing it, the loss of productivity, and the value of any data that may be corrupted or
lost must be accounted for to properly capture the amount the organization would lose
if the server were to fail for one reason or another.
The following issues should be considered when assigning values to assets:

Determining the value of assets may be useful to an organization for a variety of
reasons, including the following:

- To perform effective cost/benefit analyses
- To select specific countermeasures and safeguards
- To determine the level of insurance coverage to purchase
- To understand what exactly is at risk
- To comply with legal and regulatory requirements

Assets may be tangible (computers, facilities, supplies) or intangible (reputation, data,
intellectual property). It is usually harder to quantify the values of intangible assets, which
may change over time. How do you put a monetary value on a company's reputation? This
is not always an easy question to answer, but it is important to be able to do so.

Risk Assessment Teams

Each organization has different departments, and each department has its own
functionality, resources, tasks, and quirks. For the most effective risk assessment, an organization
must build a risk assessment team that includes individuals from many or all
departments to ensure that all of the threats are identified and addressed. The team members
may be part of management, application programmers, IT staff, systems integrators,
and operational managers—indeed, any key personnel from key areas of the organization.
This mix is necessary because if the team comprises only individuals from the IT
department, it may not understand, for example, the types of threats the accounting department
faces with data integrity issues, or how the organization as a whole would be affected if
the accounting department's data files were wiped out by an accidental or intentional act.

Asking the Right Questions

When looking at risk, it's good to keep several questions in mind. Raising these
questions helps ensure that the risk assessment team and senior management know
what is important. Team members must ask the following:

• What event could occur (threat event)?
• What could be the potential impact (risk)?
• How often could it happen (frequency)?
• What level of confidence do we have in the answers to the first three questions (certainty)?

A lot of this information is gathered through internal surveys, interviews, or workshops. Viewing threats with these questions in mind helps the team focus on the tasks at hand and assists in making the decisions more accurate and relevant.

Methodologies for Risk Assessment

The industry has different standardized methodologies for carrying out risk assessments.

Each of the individual methodologies has the same basic core components (identify vulnerabilities, associate threats, calculate risk values), but each has a specific focus. Keep in mind that the methodologies have a lot of overlapping similarities because each one has the specific goal of identifying things that could hurt the organization (vulnerabilities and threats) so that those things can be addressed (risk reduced). What make these methodologies different from each other are their unique approaches and focuses.

If you need to deploy an organization-wide risk management program and integrate it into your security program, you should follow the OCTAVE method. If you need to focus just on IT security risks during your assessment, you can follow NIST SP 800-30.

If you have a limited budget and need to carry out a focused assessment on an individual system or process, you can follow the Facilitated Risk Analysis Process. If you really want to dig into the details of how a security flaw within a specific system could cause negative ramifications, you could use Failure Modes and Effect Analysis or fault tree analysis.

NIST SP 800-30

NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments, is specific to information systems threats and how they relate to information security risks. It lays out the following steps:

1. Prepare for the assessment.
2. Conduct the assessment:
a. Identify threat sources and events.
b. Identify vulnerabilities and predisposing conditions.
c. Determine likelihood of occurrence.
d. Determine magnitude of impact.
e. Determine risk.

3. Communicate results.
4. Maintain assessment.

Or, as another example, the IT staff may not understand all the risks the employees in the warehouse would face if a natural disaster were to hit, or what it would mean to their productivity and how it would affect the organization overall. If the risk assessment team is unable to include members from various departments, it should, at the very least, make sure to interview people in each department so it fully understands and can quantify all threats.
The risk assessment team must also include people who understand the processes that are part of their individual departments, meaning individuals who are at the right levels of each department. This is a difficult task, since managers sometimes delegate any sort of risk assessment task to lower levels within the department. However, the people who work at these lower levels may not have adequate knowledge and understanding of the processes that the risk assessment team may need to deal with.

The NIST risk management methodology is mainly focused on computer systems and IT security issues. It does not explicitly cover larger organizational threat types, as in succession planning, environmental issues, or how security risks associate to business risks.
It is a methodology that focuses on the operational components of an enterprise, not necessarily the higher strategic level.

FRAP
Facilitated Risk Analysis Process (FRAP) is a second type of risk assessment methodology.
The crux of this qualitative methodology is to focus only on the systems that really need assessing, to reduce costs and time obligations. FRAP stresses prescreening activities so that the risk assessment steps are only carried out on the item(s) that needs it the most.
FRAP is intended to be used to analyze one system, application, or business process at a time. Data is gathered and threats to business operations are prioritized based upon their criticality. The risk assessment team documents the controls that need to be put

into place
to reduce the identified risks along with action plans for control
implementation efforts.
This methodology does not support the idea of calculating exploitation
probability
numbers or annualized loss expectancy values. The criticalities of the risks are
determined by the team members' experience. The author of this methodology
(Thomas
Peltier) believes that trying to use mathematical formulas for the calculation
of risk is too
confusing and time consuming. The goal is to keep the scope of the assessment
small and
the assessment processes simple to allow for efficiency and cost-effectiveness.

OCTAVE
The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
methodology was created by Carnegie Mellon University's Software Engineering
Institute
(SIE). OCTAVE is intended to be used in situations where people manage and
direct
the risk evaluation for information security within their organization. This
places the
people who work inside the organization in the power positions of being able to
make
the decisions regarding what is the best approach for evaluating the security of
their
organization. OCTAVE relies on the idea that the people working in these
environments
best understand what is needed and what kind of risks they are facing. The
individuals
who make up the risk assessment team go through rounds of facilitated workshops.
The
facilitator helps the team members understand the risk methodology and how to
apply it
to the vulnerabilities and threats identified within their specific business
units. OCTAVE
stresses a self-directed team approach.
The scope of an OCTAVE assessment is usually very wide compared to the more
focused approach of FRAP. Where FRAP would be used to assess a system or
application,
OCTAVE would be used to assess all systems, applications, and business processes
within
the organization.
The OCTAVE methodology consists of the seven processes (or steps) listed here:
1. Identify enterprise knowledge.
2. Identify operational area knowledge.
3. Identify staff knowledge.

4. Establish security requirements.
6. Perform infrastructure vulnerability evaluation.
7. Conduct multidimensional risk analysis.

8. Develop protection strategy.

FMEA
Failure Modes and Effect Analysis (FMEA) is a method for determining functions, identifying functional failures, and assessing the causes of failure and their failure effects
through a structured process. FMEA is commonly used in product development and operational environments. The goal is to identify where something is most likely going to
break and either fix the flaws that could cause this issue or implement controls to reduce
the impact of the break. For example, you might choose to carry out an FMEA on your
organization's network to identify single points of failure. These single points of failure
represent vulnerabilities that could directly affect the productivity of the network as a
whole. You would use this structured approach to identify these issues (vulnerabilities),
assess their criticality (risk), and identify the necessary controls that should be put into
place (reduce risk).
The FMEA methodology uses failure modes (how something can break or fail) and effects analysis (impact of that break or failure). The application of this process to a
chronic failure enables the determination of where exactly the failure is most likely
to occur. Think of it as being able to look into the future and locate areas that have
the potential for failure and then applying corrective measures to them before they do
become actual liabilities.
By following a specific order of steps, the best results can be maximized for an FMEA:
1. Start with a block diagram of a system or control.
2. Consider what happens if each block of the diagram fails.
3. Draw up a table in which failures are paired with their effects and an evaluation
of the effects.
4. Correct the design of the system, and adjust the table until the system is not
known to have unacceptable problems.
5. Have several engineers review the Failure Modes and Effect Analysis.

Table 2-2 is an example of how an FMEA can be carried out and documented. Although most organizations will not have the resources to do this level of detailed work
for every system and control, an organization can carry it out on critical functions and
systems that can drastically affect the organization.
FMEA was first developed for systems engineering. Its purpose is to examine the potential failures in products and the processes involved with them. This approach
proved to be successful and has been more recently adapted for use in evaluating

risk
management priorities and mitigating known threat vulnerabilities.

PART I

5. Map high-priority information assets to information infrastructure.

↟Approved by:
Date:
Revision:
Failure Effect on . . .
Failure
Mode

Failure
Cause

Component
or Functional
Assembly

Next Higher
Assembly

Item Identification

Function

IPS application
content filter

Inline
perimeter
protection

Fails to
close

Traffic
overload

Single point of IPS blocks
failure Denial of ingress traffic
service
stream

IPS is
brought
down

Health check
status sent
to console
and e-mail