1 RISK MANAGEMENT AND PRIVACY

Information security is the art and practice of managing the confidentiality, integrity, and availability risks associated with information. As you begin your exploration of the field, it is best to start with that in mind. In this chapter, we'll explore the process that security professionals use to identify, assess, and manage the risks facing their organizations.

CIA AND DAD TRIADS

Security professionals, tasked with protecting the information assets of an organization, typically think of their responsibilities in three realms: confidentiality, integrity, and availability (CIA). Adversaries, seeking to disrupt an organization's security, have three corresponding goals in mind: disclosure, alteration, and denial (DAD). These models, shown in Figure 1-1, are known as the CIA and DAD triads and are the classic models embraced by security professionals around the world.

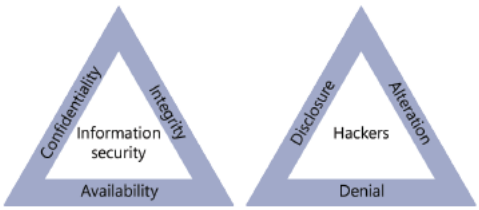


FIGURE 1-1 The CIA and DAD triads are the classic models of information security principles.

CONFIDENTIALITY AND DISCLOSURE

The goal of confidentiality is to prevent unauthorized access to sensitive information. Quite simply, it is to keep secrets secret. Achieving confidentiality first requires that an organization classify its data, identifying which information assets are worthy of protection and the appropriate level of protection for each. For example, an organization might consider design documents for an unreleased product highly sensitive due to their competitive value. On the other hand, the internal phone book might be considerably less sensitive. Organizing confidential information into different data classifications allows security professionals to design appropriate controls, focusing scarce resources on the most sensitive data.

Adversaries, on the other hand, pursue the goal of disclosure, gaining access to sensitive information without permission. They may want to use this information for personal gain, to embarrass the organization publicly, or to simply make information freely available.

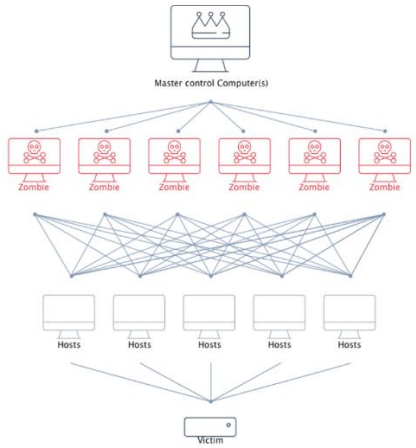
The WikiLeaks website, made famous by disclosures of sensitive US government information by Bradley Manning in 2010 and Edward Snowden in 2013, is dedicated to the disclosure of information that governments and corporations may find embarrassing.

INTEGRITY AND ALTERATION

Security professionals also pursue the goal of integrity, ensuring that information is only modified or deleted by authorized means. Protecting the integrity of information requires controls against deliberate alteration by adversaries such as an employee seeking to modify his payroll information without permission. It also requires protection against unintentional alteration, such as the corruption of data due to a software or hardware failure.

AVAILABILITY AND DENIAL

It’s not sufficient for security professionals to provide confidentiality and integrity controls. These must be supplemented with availability protection that ensures that authorized individuals have access to information when needed. Denial attacks occur when an adversary is able to successfully interrupt the availability of information, such as through a denial of service (DoS) attack. Adversaries might also attempt to harness many systems around the world to simultaneously perform a denial attack by using a technique known as distributed denial of service (DDoS).



ANALYZING RISK

We operate in a world full of risks. If you left your home and drove to your office this morning, you encountered a large number of risks. You could have been involved in an automobile accident, encountered a train delay, or been struck by a bicycle on the sidewalk. We're aware of these risks in the back of our minds, but we don't let them paralyze us. Instead, we take simple precautions to help manage the risks that we think have the greatest potential to disrupt our lives.

In an enterprise risk management (ERM) program, organizations take a formal approach to risk analysis that begins with identifying risks, continues with determining the severity of each risk, and then results in adopting one or more risk management strategies to address each risk.

Before we move too deeply into the risk assessment process, let's define a few important terms that we'll use during our discussion:
Threats are any possible events that might have an adverse impact on the confidentiality, integrity, and/or availability of our information or information systems.
Vulnerabilities are weaknesses in our systems or controls that could be exploited by a threat.

Risks occur at the intersection of a vulnerability and a threat that might exploit that vulnerability. A threat without a corresponding vulnerability does not pose a risk, nor does a vulnerability without a corresponding threat.

Figure 1.1 illustrates this relationship between threats, vulnerabilities, and risks.

Consider the example from earlier of walking down the sidewalk on your way to work. The fact that you are on the sidewalk without any protection is a vulnerability. A bicycle speeding down that

sidewalk is a threat. The result of this combination of factors is that you are at risk of being hit by the bicycle on the sidewalk. If you remove the vulnerability by parking in a garage beneath your building, you are no longer at risk for that particular threat. Similarly, if the city erects barriers that prevent bicycles from entering the sidewalk, you are also no longer at risk.

Let's consider another example drawn from the cybersecurity domain. Organizations regularly conduct vulnerability scans designed to identify potential vulnerabilities in their environment. One of these scans might identify a server that exposes TCP port 22 to the world, allowing brute-force SSH attempts by an attacker. Exposing port 22 presents a vulnerability to a brute-force attack. An attacker with a brute-force scanning tool presents a threat. The combination of the port exposure and the existence of attackers presents a risk.

In this case, you don't have any way to eliminate attackers, so you can't really address the threat, but you do have control over the services running on your systems. If you shut down the SSH service and close port 22, you eliminate the vulnerability and, therefore, also eliminate the risk.

Of course, we can't always completely eliminate a risk because it isn't always feasible to shut down services. We might decide instead to take actions that reduce the risk. We'll talk more about those options when we get to risk management strategies later in this chapter.

RISK IDENTIFICATION

The risk identification process requires identifying the threats and vulnerabilities that exist in your operating environment. These risks may come from a wide variety of sources ranging from hackers to hurricanes.

External risks are those risks that originate from a source outside the organization. This is an extremely broad category of risk, including cybersecurity adversaries, malicious code, and natural disasters, among many other types of risk.

Internal risks are those risks that originate from within the organization. They include malicious insiders, mistakes made by authorized users, equipment failures, and similar risks.

Multiparty risks are those that impact more than one organization. For example, a power outage to a city block is a multiparty risk because it affects all of the buildings on that block. Similarly, the compromise of an SaaS provider's database is a multiparty risk because it compromises the information of many different customers of the SaaS provider.

Legacy systems pose a unique type of risk to organizations. These outdated systems often do not receive security updates and cybersecurity professionals must take extraordinary measures to protect them against unpatchable vulnerabilities.

Intellectual property (IP) theft risks occur when a company possesses trade secrets or other proprietary information which, if disclosed, could compromise the organization's business advantage.

Software compliance/licensing risks occur when an organization licenses software from a vendor and intentionally or accidentally runs afoul of usage limitations that expose the customer to financial and legal risk.

RISK CALCULATION

Not all risks are equal. Returning to the example of a pedestrian on the street, the risk of being hit by a bicycle is far more worrisome than the risk of being struck down by a meteor. That makes intuitive

sense, but let's explore the underlying thought process that leads to that conclusion. It's a process called risk calculation.

When we evaluate any risk, we do so by using two different factors:

The likelihood of occurrence, or probability, that the risk will occur. We might express this as the percent chance that a threat will exploit a vulnerability over a specified period of time, such as within the next year.

The magnitude of the impact that the risk will have on the organization if it does occur. We might express this as the financial cost that we will incur as the result of a risk, although there are other possible measures.

Using these two factors, we can assign each risk a conceptual score by combining the probability and the magnitude. This leads many risk analysts to express the severity of a risk using the formula:

Risk Severity = Likelihood * Impact

It's important to point out that this equation does not always have to be interpreted literally. Although you may wind up multiplying these values together in some risk assessment processes, it's best to think of this conceptually as combining the likelihood and impact to determine the severity of a risk.

When we assess the risks of being struck by a bicycle or a meteor on the street, we can use these factors to evaluate the risk severity. There might be a high probability that we will be struck by a bicycle. That type of accident might have a moderate magnitude, leaving us willing to consider taking steps to reduce our risk. Being struck by a meteor would clearly have a catastrophic magnitude of impact, but the probability of such an incident is incredibly unlikely, leading us to acknowledge the risk and move on without changing our behavior.

The laws and regulations facing an industry may play a significant role in determining the impact of a risk. For example, an organization subject to the European Union's GDPR faces significant fines if they have a data breach affecting the personal information of EU residents. The size of these fines would factor significantly into the impact assessment of the risk of a privacy breach. Organizations must, therefore, remain current on the regulations that affect their risk posture.

RISK ASSESSMENT

Risk assessments are a formalized approach to risk prioritization that allows organizations to conduct their reviews in a structured manner. Risk assessments follow two different analysis methodologies:

Quantitative risk assessments use numeric data in the analysis, resulting in assessments that allow the very straightforward prioritization of risks.

Qualitative risk assessments substitute subjective judgments and categories for strict numerical analysis, allowing the assessment of risks that are difficult to quantify.

As organizations seek to provide clear communication of risk factors to stakeholders, they often combine elements of quantitative and qualitative risk assessments. Let's review each of these approaches.

QUANTITATIVE RISK ASSESSMENT

Most quantitative risk assessment processes follow a similar methodology that includes the following steps:

Determine the asset value (AV) of the asset affected by the risk. This asset value (AV) is expressed in dollars, or other currency, and may be determined using the cost to acquire the asset, the cost to replace the asset, or the depreciated cost of the asset, depending on the organization's preferences.

Determine the likelihood that the risk will occur. Risk analysts consult subject matter experts and determine the likelihood that a risk will occur in a given year. This is expressed as the number of times the risk is expected each year and is described as the annualized rate of occurrence (ARO). A risk that is expected to occur twice a year has an ARO of 2.0, whereas a risk that is expected once every one hundred years has an ARO of 0.01.

Determine the amount of damage that will occur to the asset if the risk materializes. This is known as the exposure factor (EF) and is expressed as the percentage of the asset expected to be damaged. The exposure factor of a risk that would completely destroy an asset is 100 percent, whereas a risk that would damage half of an asset has an EF of 50 percent.

Calculate the single loss expectancy. The single loss expectancy (SLE) is the amount of financial damage expected each time a risk materializes. It is calculated by multiplying the AV by the EF.

Calculate the annualized loss expectancy. The annualized loss expectancy (ALE) is the amount of damage expected from a risk each year. It is calculated by multiplying the SLE and the ARO.

It's important to note that these steps assess the quantitative scale of a single risk: that is one combination of a threat and a vulnerability. Organizations conducting quantitative risk assessments would repeat this process for each threat/vulnerability combination.

Let's walk through an example of a quantitative risk assessment. Imagine that you are concerned about the risk associated with a denial-of-service (DoS) attack against your email server. Your organization uses that server to send email messages to customers offering products for sale. It generates $1,000 in sales per hour that it is in operation. After consulting threat intelligence sources, you believe that a DoS attack is likely to occur three times a year and last for three hours before you are able to control it.

The asset in this case is not the server itself, because the server will not be physically damaged. The asset is the ability to send email and you have already determined that it is worth $1,000 per hour. The asset value for three hours of server operation is, therefore, $3,000.

Your threat intelligence estimates that the risk will occur three times per year, making your annualized rate of occurrence 3.0.

After consulting your email team, you believe that the server would operate at 10 percent capacity during a DoS attack, as some legitimate messages would get out. Therefore, your exposure factor is 90 percent, because 90 percent of the capacity would be consumed by the attack.

Your single loss expectancy is calculated by multiplying the asset value ($3,000) by the exposure factor (90 percent) to get the expected loss during each attack. This gives you an SLE of $2,700.

Your annualized loss expectancy is the product of the SLE ($2,700) and the ARO (3.0), or $8,100.

Organizations can use the ALEs that result from a quantitative risk assessment to prioritize their remediation activities and determine the appropriate level of investment in controls that mitigate risks. For example, it would not normally make sense (at least in a strictly financial sense) to spend more than the ALE on an annual basis to protect against a risk. In the previous example, if a DoS

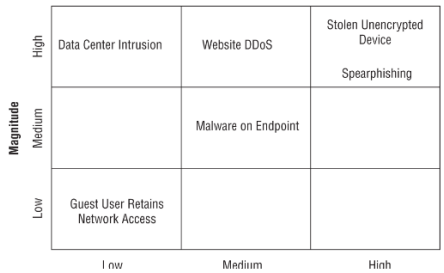
prevention service would block all of those attacks, it would make financial sense to purchase it if the cost is less than $8,100 per year.

QUALITATIVE RISK ASSESSMENT

Quantitative techniques work very well for evaluating financial risks and other risks that can be clearly expressed in numeric terms. Many risks, however, do not easily lend themselves to quantitative analysis. For example, how would you describe reputational damage, public health and safety, or employee morale in quantitative terms? You might be able to draw some inferences that tie these issues back to financial data, but the bottom line is that quantitative techniques simply aren't well suited to evaluating these risks.

Qualitative risk assessment techniques seek to overcome the limitations of quantitative techniques by substituting subjective judgment for objective data. Qualitative techniques still use the same probability and magnitude factors to evaluate the severity of a risk but do so using subjective categories. For example, Figure 1.2 shows a simple qualitative risk assessment that evaluates the probability and magnitude of several risks on a subjective Low/Medium/High scale. Risks are placed on this chart based on the judgments made by subject matter experts.

Although it's not possible to directly calculate the financial impact of risks that are assessed using qualitative techniques, this risk assessment scale makes it possible to prioritize risks. For example, reviewing the risk assessment in Figure 1.2, we can determine that the greatest risks facing this organization are stolen unencrypted devices and spearphishing attacks. Both of these risks share a high probability and high magnitude of impact. If we're considering using funds to add better physical security to the data center, this risk assessment informs us that our time and money would likely be better spent on full disk encryption for mobile devices and a secure email gateway.



SUPPLY CHAIN ASSESSMENT

When evaluating the risks to your organization, don't forget about the risks that occur based on third-party relationships. You rely on many different vendors to protect the confidentiality, integrity, and availability of your data. Performing vendor due diligence is a crucial security responsibility.

For example, how many cloud service providers handle your organization's sensitive information? Those vendors become a crucial part of your supply chain from both operational and security perspectives. If they don't have adequate security controls in place, your data is at risk.

Similarly, the hardware that you use in your organization comes through a supply chain as well. How certain are you that it wasn't tampered with on the way to your organization? Documents leaked by former NSA contractor Edward Snowden revealed that the U.S. government intercepted hardware shipments to foreign countries and implanted malicious code deep within their hardware. Performing hardware source authenticity assessments validates that the hardware you received was not tampered with after leaving the vendor.

MANAGING RISK

With a completed risk assessment in hand, organizations can then turn their attention to addressing those risks. Risk management is the process of systematically addressing the risks facing an organization. The risk assessment serves two important roles in the risk management process:

The risk assessment provides guidance in prioritizing risks so that the risks with the highest probability and magnitude are addressed first.

Quantitative risk assessments help determine whether the potential impact of a risk justifies the costs incurred by adopting a risk management approach.

Risk managers should work their way through the risk assessment and identify an appropriate management strategy for each risk included in the assessment. They have four strategies to choose from: risk mitigation, risk avoidance, risk transference, and risk acceptance. In the next several sections, we discuss each of these strategies using two examples.

First, we discuss the financial risk associated with the theft of a laptop from an employee. In this example, we are assuming that the laptop does not contain any unencrypted sensitive information. The risk that we are managing is the financial impact of losing the actual hardware.

Second, we discuss the business risk associated with a distributed denial-of-service (DDoS) attack against an organization's website.

We use these two scenarios to help you understand the different options available when selecting a risk management strategy and the trade-offs involved in that selection process.

RISK MITIGATION

Risk mitigation is the process of applying security controls to reduce the probability and/or magnitude of a risk. Risk mitigation is the most common risk management strategy and the vast majority of the work of security professionals revolves around mitigating risks through the design, implementation, and management of security controls. Many of these controls involve engineering tradeoffs between functionality, performance, and security.

When you choose to mitigate a risk, you may apply one security control or a series of security controls. Each of those controls should reduce the probability that the risk will materialize, the magnitude of the risk should it materialize, or both the probability and magnitude.

In our first scenario, we are concerned about the theft of laptops from our organization. If we want to mitigate that risk, we could choose from a variety of security controls. For example, purchasing cable locks for laptops might reduce the probability that a theft will occur.

FIGURE 17.3 (a) STOP tag attached to a device. (b) Residue remaining on device after attempted removal of a STOP tag.

We could also choose to purchase a device registration service that provides tamperproof registration tags for devices, such as the STOP tags shown in Figure 17.3. These tags provide a prominent warning to potential thieves when attached to a device, as shown in Figure 17.3(a). This serves as a deterrent to theft, reducing the probability that the laptop will be stolen in the first place. If a thief does steal the device and removes the tag, it leaves the permanent residue, shown in Figure 17.3(b). Anyone finding the device is instructed to contact the registration vendor for instructions, reducing the potential impact of the theft if the device is returned.

In our second scenario, a DDoS attack against an organization's website, we could choose among several mitigating controls. For example, we could simply purchase more bandwidth and server capacity, allowing us to absorb the bombardment of a DDoS attack and thus reducing the impact of an attack. We could also choose to purchase a third-party DDoS mitigation service that prevents the traffic from reaching our network in the first place, thus reducing the probability of an attack.

RISK AVOIDANCE

Risk avoidance is a risk management strategy where we change our business practices to completely eliminate the potential that a risk will materialize. Risk avoidance may initially seem like a highly desirable approach. After all, who wouldn't want to eliminate the risks facing their organization? There is, however, a major drawback. Risk avoidance strategies typically have a serious detrimental impact on the business.

For example, consider the laptop theft risk discussed earlier in this chapter. We could adopt a risk avoidance strategy and completely eliminate the risk by not allowing employees to purchase or use laptops. This approach is unwieldy and would likely be met with strong opposition from employees and managers due to the negative impact on employee productivity.

Similarly, we could avoid the risk of a DDoS attack against the organization's website by simply shutting down the website. If there is no website to attack, there's no risk that a DDoS attack can affect the site. But it's highly improbable that business leaders will accept shutting down the website as a viable approach. In fact, you might consider being driven to shut down your website to avoid DDoS attacks as the ultimate denial-of-service attack!

RISK TRANSFERENCE

Risk transference shifts some of the impact of a risk from the organization experiencing the risk to another entity. The most common example of risk transference is purchasing an insurance policy that covers a risk. When purchasing insurance, the customer pays a premium to the insurance carrier. In exchange, the insurance carrier agrees to cover losses from risks specified in the policy.

In the example of laptop theft, property insurance policies may cover the risk. If an employee's laptop is stolen, the insurance policy would provide funds to cover either the value of the stolen device or the cost to replace the device, depending on the type of coverage.

It's unlikely that a property insurance policy would cover a DDoS attack. In fact, many general business policies exclude all cybersecurity risks. An organization seeking insurance coverage against this type of attack should purchase cybersecurity insurance, either as a separate policy or as a rider on an existing business insurance policy. This coverage would repay some or all of the cost of recovering operations and may also cover lost revenue during an attack.

RISK ACCEPTANCE

Risk acceptance is the final risk management strategy and it boils down to deliberately choosing to take no other risk management strategy and to simply continue operations as normal in the face of the risk. A risk acceptance approach may be warranted if the cost of mitigating a risk is greater than the impact of the risk itself.

In our laptop theft example, we might decide that none of the other risk management strategies are appropriate. For example, we might feel that the use of cable locks is an unnecessary burden and that theft recovery tags are unlikely to work, leaving us without a viable risk mitigation strategy. Business leaders might require that employees have laptop devices, taking risk avoidance off the table. And the cost of a laptop insurance policy might be too high to justify. In that case, we might decide that we will simply accept the risk and cover the cost of stolen devices when thefts occur. That's risk acceptance.

In the case of the DDoS risk, we might go through a similar analysis and decide that risk mitigation and transference strategies are too costly. In the event we continue to operate the site, we might do so accepting the risk that a DDoS attack could take the site down.

RISK ANALYSIS

As you work to manage risks, you will implement controls designed to mitigate those risks. There are a few key terms that you can use to describe different states of risk that you should know :

- The inherent risk facing an organization is the original level of risk that exists before implementing any controls. Inherent risk takes its name from the fact that it is the level of risk inherent in the organization's business.
- The residual risk is the risk that remains after an organization implements controls designed to mitigate, avoid, and/or transfer the inherent risk.
- An organization's risk appetite is the level of risk that it is willing to accept as a cost of doing business.

These three concepts are connected by the way that an organization manages risk. An organization begins with its inherent risk and then implements risk management strategies to reduce that level of risk. It continues doing so until the residual risk is at or below the organization's risk appetite.

CONTROL RISK

The world of public accounting brings us the concept of control risk. Control risk is the risk that arises from the potential that a lack of internal controls within the organization will cause a material misstatement in the organization's financial reports. Information technology risks can contribute to control risks if they jeopardize the integrity or availability of financial information. For this reason, financial audits often include tests of the controls protecting financial systems.

Organizations can implement these concepts only if they have a high degree of risk awareness. They must understand the risks they face and the controls they can implement to manage those risks. They must also conduct regular risk control assessments and self-assessments to determine whether those controls continue to operate effectively.

As risk managers work to track and manage risks, they must communicate their results to other risk professionals and business leaders. The risk register is the primary tool that risk management professionals use to track risks facing the organization. Figure 1.4 shows an excerpt from a risk register used to track IT risks in higher education.

ID	Risk Statement	Risk Causes	Risk Impacts	Likelihood	Impact	Score
20	No coordinated vetting and review process for third-party or cloud-computing services used to store, process, or transmit institutional data	Lack of senior management support; lack of communication of central vetting process to staff/employees; failure to understand the need to protect institutional data	Multiple redundant services in place (inefficient and costly for the institution); institution unaware who its business partners are; institution unaware if institutional data are held by third parties; institution unable to ensure that third parties are following compliance requirements	1	2	2
21	Failure to create and maintain sufficient and current policies and standards to protect the confidentiality, integrity, and availability of institutional data and IT resources (e.g., hardware, devices, data, and software)	Lack of senior management support; failure to understand information security concepts; lack of funding to support policy development activities; lack of funding for training; lack of user training	Improper use of university IT systems and institutional data; failure of users to protect critical institutional data when using IT resources (leading to data breach); institution subject to regulatory violations and fines; institutional reputation loss; poor perception/reputation of IT	2	3	6
22	Data breach or leak of sensitive information (e.g., academic, business, or research data)	Lack of senior management support; complex regulatory environments impacting higher education IT systems and data (e.g., FERPA, HIPAA, GLBA, PCI, accessibility, export controls, etc.); complexity of IT systems, infrastructure, and services; lack of funding for data handling training; lack of user training; intentional user malfeasance; unintentional user error; hacking or infiltration by third parties	Institution subject to regulatory violations and fines; costs of breach notification; costs of redress for individuals; loss of alumni donations; loss of research data; costs to mitigate underlying breach event; institutional reputation loss; poor perception/reputation of IT	3	3	9

FIGURE 1.4 Risk register excerpt

Source: EDUCAUSE IT Risk Register (library.educause.edu/resources/2015/10/it-risk-register)

The risk register is a lengthy document that often provides far too much detail for business leaders. When communicating risk management concepts to senior leaders, risk professionals often use a risk matrix, or heat map, such as the one shown in Figure 1.5. This approach quickly summarizes risks and allows senior leaders to quickly focus on the most significant risks facing the organization.

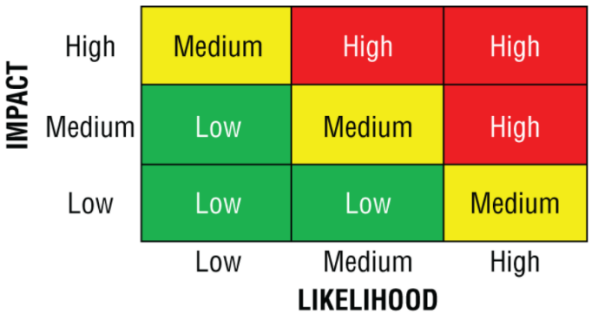


FIGURE 17.5 Risk matrix

DISASTER RECOVERY PLANNING

No matter how many controls we put in place, the reality is that disasters will sometimes strike our organization and cause disruptions. Disaster recovery planning (DRP) is the discipline of developing plans to recover operations as quickly as possible in the face of a disaster. The disaster recovery planning process creates a formal, broad disaster recovery plan for the organization and, when required, develops specific functional recovery plans for critical business functions. The goal of these plans is to help the organization recover normal operations as quickly as possible in the wake of a disruption.

DISASTER TYPES

Disasters of any type may strike an organization. When we first hear the word “disaster,” we often immediately conjure up images of hurricanes, floods, and other natural environmental disasters. However, disasters may be of man-made origin and may come as a result of forces external to the organization, as well as internal risks. From a disaster recovery planning perspective, a disaster is any event that has the potential to disrupt an organization's business. The occurrence of a disaster triggers the activation of the organization's disaster recovery plan.

As part of the DRP process, organizations should conduct site risk assessments for each of their facilities. These risk assessments should seek to identify and prioritize the risks posed to the facilitate

by a disaster, including both internal and external risks from both environmental and man-made disasters.

BUSINESS IMPACT ANALYSIS

The business impact analysis (BIA) is a formal process designed to identify the mission essential functions within an organization and facilitate the identification of the critical systems that support those functions.

There are four key metrics used in the BIA process that you should understand.

The Mean Time Between Failures (MTBF) is a measure of the reliability of a system. It is the expected amount of time that will elapse between system failures. For example, if the MTBF is six months, you can expect that the system will fail once every six months, on average.

The Mean Time to Repair (MTTR) is the average amount of time to restore a system to its normal operating state after a failure.

The Recovery Time Objective (RTO) is the amount of time that the organization can tolerate a system being down before it is repaired. The service team is meeting expectations when the time to repair is less than the RTO.

The Recovery Point Objective (RPO) is the amount of data that the organization can tolerate losing during an outage.

Each of these metrics allows the organization to evaluate the impact of different risks on its operations and the acceptability of the state of its disaster recovery controls.

As organizations evaluate the state of their environment, they should pay particular attention to single points of failure. These are systems, devices, or other components that, if they fail, would cause an outage. For example, if a server only has one power supply, the failure of that power supply would bring down the server, making it a single point of failure. Adding a redundant power supply to the server resolves that single point of failure. Similarly, if that server is the only server providing the organization's web page, the server then becomes a single point of failure. Adding a second server to a cluster resolves that single point of failure.

PRIVACY

Cybersecurity professionals are responsible for protecting the confidentiality, integrity, and availability of all information under their care. This includes personally identifiable information (PII) that, if improperly disclosed, would jeopardize the privacy of one or more individuals.

When privacy breaches occur, they clearly have a negative impact on the individuals whose information was lost in the breach. Those individuals may find themselves exposed to identity theft and other personal risks. Privacy breaches also have organizational consequences for the business that loses control of personal information. These consequences may include reputational damage, fines, and the loss of important intellectual property (IP) that may now fall into the hands of a competitor.

Organizations seeking to codify their privacy practices may adopt a privacy notice that outlines their privacy commitments. In some cases, laws or regulations may require that the organization adopt a privacy notice. In addition, organizations may include privacy statements in their terms of agreement with customers and other stakeholders.

SENSITIVE INFORMATION INVENTORY

Organizations often deal with many different types of sensitive and personal information. The first step in managing this sensitive data is developing an inventory of the types of data maintained by the organization and the places where it is stored, processed, and transmitted.

Organizations should include the following types of information in their inventory:

Personally identifiable information (PII) includes any information that uniquely identifies an individual person, including customers, employees, and third parties.

Protected health information (PHI) includes medical records maintained by healthcare providers and other organizations that are subject to the Health Insurance Portability and Accountability Act (HIPAA).

Financial information includes any personal financial records maintained by the organization.

Government information maintained by the organization may be subject to other rules, including the data classification requirements discussed in the next section

Once the organization has an inventory of this sensitive information, it can begin to take steps to ensure that it is appropriately protected from loss or theft.

INFORMATION CLASSIFICATION

Information classification programs organize data into categories based on the sensitivity of the information and the impact on the organization should the information be inadvertently disclosed. For example, the U.S. government uses the following four major classification categories:

Top Secret information requires the highest degree of protection. The unauthorized disclosure of Top Secret information could reasonably be expected to cause exceptionally grave damage to national security.

Secret information requires a substantial degree of protection. The unauthorized disclosure of Secret information could reasonably be expected to cause serious damage to national security.

Confidential information requires some protection. The unauthorized disclosure of Confidential information could reasonably be expected to cause identifiable damage to national security.

Unclassified information is information that does not meet the standards for classification under the other categories. Information in this category is still not publicly releasable without authorization.

Businesses generally don't use the same terminology for their levels of classified information. Instead, they might use more friendly terms, such as Highly Sensitive, Sensitive, Internal, and Public.

Become familiar with these examples that are commonly used in business:

- Public
- Private
- Sensitive
- Confidential
- Critical
- Proprietary

It's important to understand that there are no “official” classification levels in business. Each of these terms may be used differently between organizations and it is likely that different firms may use these terms for different purposes. It's very important to review your organization's classification policy and understand the different levels in use and their meanings.

FIGURE 1.6 Cover sheets used to identify classified U.S. government information

Data classification allows organizations to clearly specify the security controls required to protect information with different levels of sensitivity. For example, the U.S. government requires the use of brightly colored cover sheets, such as those shown in Figure 17.6, to identify classified information in printed form.

DATA ROLES AND RESPONSIBILITIES

One of the most important things that we can do to protect our data is to create clear data ownership policies and procedures. Using this approach, the organization designates specific senior executives as the data owners for different data types. For example, the vice president of Human Resources might be the data owner for employment and payroll data, whereas the vice president for Sales might be the data owner for customer information.

Clear lines of data ownership place responsibility for data in the hands of executives who best understand the impact of decisions about that data on the business. They don't make all of these decisions in isolation, however. Data owners delegate some of their responsibilities to others in the organization and also rely on advice from subject matter experts, such as cybersecurity analysts and data protection specialists.

You should be familiar with other important data privacy roles:

- Data controllers are the entities who determine the reasons for processing personal information and direct the methods of processing that data. This term is used primarily in European law and it serves as a substitute for the term data owner to avoid a presumption that anyone who collects data has an ownership interest in that data.
- Data stewards are individuals who carry out the intent of the data controller and are delegated responsibility from the controller.
- Data custodians are individuals or teams who do not have controller or stewardship responsibility but are responsible for the secure safekeeping of information. For example, a data controller might delegate responsibility for securing PII to an information security team. In that case, the information security team serves as a data custodian.
- Data processors are service providers that process personal information on behalf of a data controller. For example, a credit card processing service might be a data processor for a retailer. The retailer retains responsibility as the data controller but uses the service as a data processor.

- Information Lifecycle
- Data protection should continue at all stages of the information lifecycle, from the time the data is originally collected until the time it is eventually disposed.

At the early stages of the data lifecycle, organizations should practice data minimization, where they collect the smallest possible amount of information necessary to meet their business requirements. Information that is not necessary should either be immediately discarded or, better yet, not collected in the first place.

Although information remains within the care of the organization, the organization should practice purpose limitation. This means that information should be used only for the purpose that it was originally collected and that was consented to by the data subjects.

At the end of the lifecycle, the organization should implement data retention standards that guide the end of the data lifecycle. Data should only be kept for as long as it remains necessary to fulfill the purpose for which it was originally collected. At the conclusion of its lifecycle, data should be securely destroyed.

PRIVACY ENHANCING TECHNOLOGIES

If we can't completely remove data from a dataset, we can often transform it into a format where the original sensitive information is anonymized. Although true anonymization may be quite difficult to achieve, we can often use pseudo-anonymization techniques, such as de-identification.
The de-identification process removes the ability to link data back to an individual, reducing its sensitivity.

An alternative to de-identifying data is transforming it into a format where the original information can't be retrieved. This is a process called data obfuscation and we have several tools at our disposal to assist with it.

Hashing uses a hash function to transform a value in our dataset to a corresponding hash value. If we apply a strong hash function to a data element, we may replace the value in our file with the hashed value.

Tokenization replaces sensitive values with a unique identifier using a lookup table. For example, we might replace a widely known value, such as a student ID, with a randomly generated 10-digit number. We'd then maintain a lookup table that allows us to convert those back to student IDs if we need to determine someone's identity. Of course, if you use this approach, you need to keep the lookup table secure!

Data masking partially redacts sensitive information by replacing some or all of sensitive fields with blank characters. For example, we might replace all but the last four digits of a credit card number with X's or *'s to render the card number unreadable.

Although it isn't possible to retrieve the original value directly from the hashed value, there is one major flaw to this approach. If someone has a list of possible values for a field, they can conduct something called a rainbow table attack. In this attack, the attacker computes the hashes of those candidate values and then checks to see if those hashes exist in your data file.

For example, imagine that we have a file listing all the students at our college who have failed courses but we hash their student IDs. If an attacker has a list of all students, they can compute the hash values of all student IDs and then check to see which hash values are on the list. For this reason, hashing should only be used with caution.

PRIVACY AND DATA BREACH NOTIFICATION

In the unfortunate event of a data breach, the organization should immediately activate its cybersecurity incident response plan.

Organizations may also have a responsibility under national and regional laws to make public notifications and disclosures in the wake of a data breach. This responsibility may be limited to notifying the individuals involved or, in some cases, may require notification of government regulators and/or the news media.

In the United States, every state has a data breach notification law with different requirements for triggering notifications. The European Union's GDPR also includes a breach notification requirement. The U.S. lacks a federal law requiring broad notification for all security breaches but does have industry-specific laws and requirements that require notification in some circumstances.

The bottom line is that breach notification requirements vary by industry and jurisdiction and an organization experiencing a breach may be required to untangle many overlapping requirements. For this reason, organizations experiencing a data breach should consult with an attorney who is well versed in this field.

SUMMARY

Cybersecurity efforts are all about risk management. In this chapter, you learned about the techniques that cybersecurity analysts use to identify, assess, and manage a wide variety of risks. You learned about the differences between risk mitigation, risk avoidance, risk transference, and risk acceptance and when it is appropriate to use each. You also learned how the disaster recovery planning process can help prevent disruptions to a business and the role of security professionals in protecting the privacy of personally identifiable information.