Availability

Reliability

Recoverability

Solution

Enterprise high
availability

Server-level
management

Business
continuity planning

Objective

Achieve and maintain
the chosen availability
level of the enterprise’s
IT infrastructure

Emphasis

Technology

Focus

Provide an effective plan
Effectively manage and
control the IT infrastructure to minimize downtime of
key processes in the
to improve the overall
event of a major disruption
operational reliability

Processes

Proactive and
preventive

People

Response and
recovery

Preplanned procedures allow an organization to

- Provide an immediate and appropriate response to emergency situations
- Protect lives and ensure safety
- Reduce business impact
- Resume critical business functions
- Work with outside vendors and partners during the recovery period
- Reduce confusion during a crisis
- Ensure survivability of the organization
- Get “up and running” quickly after a disaster

PART I

Certain characteristics run through many of the chapters in this book: availability, integrity, and confidentiality. Here, we point out that integrity and confidentiality must be considered not only in everyday procedures but also in those procedures undertaken immediately after a disaster or disruption. For instance, it may not be appropriate to leave a server that holds confidential information in one building while everyone else moves to another building. Equipment that provides secure VPN connections may be destroyed and the team might respond by focusing on enabling remote access functionality while forgetting about the needs of encryption. In most situations the organization is purely focused on getting back up and running, thus focusing on functionality. If security is not integrated and implemented properly, the effects of the physical disaster can be amplified as threat actors come in and steal sensitive information. Many times an organization is much more vulnerable after a disaster hits, because the security services used to protect it may be unavailable or operating at a reduced capacity. Therefore, it is important that if the organization has secret stuff, it stays secret.

Availability is one of the main themes behind business continuity planning, in that it ensures that the resources required to keep the business going will continue to be available to the people and systems that rely upon them. This may mean backups need to be done religiously and that redundancy needs to be factored into the architecture of the systems, networks, and operations. If communication lines are disabled or if a service is rendered unusable for any significant period of time, there must be a quick and tested way of establishing alternative communications and services. We will be diving into the many ways organizations can implement availability solutions for continuity and recovery purposes throughout this section.

When looking at business continuity planning, some organizations focus mainly on backing up data and providing redundant hardware. Although these items are extremely important, they are just small pieces of the organization’s overall operations pie. Hardware and computers need people to configure and operate them, and data is usually not useful unless it is accessible by other systems and possibly outside entities. Thus, a larger picture of how the various processes within an organization work together needs to be understood.

Planning must include getting the right people to the right places, documenting the necessary configurations, establishing alternative communications channels (voice and data), providing power, and making sure all dependencies are properly understood and taken into account.

It is also important to understand how automated tasks can be carried out manually, if necessary, and how business processes can be safely altered to keep the operation of the organization going. This may be critical in ensuring the organization survives the event with the least impact to its operations. Without this type of vision and planning, when a disaster hits, an organization could have its backup data and redundant servers physically available at the alternative facility, but the people responsible for activating them may be standing around in a daze, not knowing where to start or how to perform in such a different environment.

Standards and Best Practices

Although no specific scientific equation must be followed to create continuity plans, certain best practices have proven themselves over time. The National Institute of Standards and Technology is responsible for developing best practices and standards as they pertain to U.S. government and military environments. It is common for NIST to document the requirements for these types of environments, and then everyone else in the industry uses NIST’s documents as guidelines. So these are “musts” for U.S. government organizations and “good to have” for other, nongovernment entities.

NIST outlines the following steps in SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems:

1. Develop the continuity planning policy statement. Write a policy that provides the guidance necessary to develop a BCP and that assigns authority to the necessary roles to carry out these tasks.
2. Conduct the business impact analysis (BIA). Identify critical functions and systems and allow the organization to prioritize them based on necessity. Identify vulnerabilities and threats, and calculate risks.
3. Identify preventive controls. Once threats are recognized, identify and implement controls and countermeasures to reduce the organization’s risk level in an economical manner.
4. Create contingency strategies. Formulate methods to ensure systems and critical functions can be brought online quickly.
5. Develop an information system contingency plan. Write procedures and guidelines for how the organization can still stay functional in a crippled state.
6. Ensure plan testing, training, and exercises. Test the plan to identify deficiencies in the BCP, and conduct training to properly prepare individuals on their expected tasks.
7. Ensure plan maintenance. Put in place steps to ensure the BCP is a living document that is updated regularly.

Continuity policy

- Integrate law and regulation requirements
- Define the scope, goals, and roles
- Management approves policy

BIA

- Identify critical functions
- Identify critical resources
- Calculate MTD for resources
- Identify threats
- Calculate risks
- Identify backup solutions

Develop
BCP
- Document
- Procedures
- Recovery solutions
- Roles and tasks
- Emergency
response

Identify preventive
controls

Create contingency
strategies

- Implement controls
- Mitigate risk

- Business processes
- Facility
- Supply and
technology
- User and user
environment
- Data

Exercise,
test, and drill
- Test plan
- Improve plan
- Train employees

Maintain
BCP
- Integrate into change
control process
- Assign responsibility
- Update plan
- Distribute after
updating

Since BCM is so critical, it is actually addressed by other standards-based organizations,
listed here:
ISO/IEC 27031:2011 Guidelines for information and communications technology readiness for business continuity. This ISO/IEC standard is a component of the overall
ISO/IEC 27000 series.
ISO 22301:2019 International standard for business continuity management systems.
The specification document against which organizations will seek certification.
Business Continuity Institute’s Good Practice Guidelines (GPG) Represents the consensus view of an international group of BC practitioners. As of this writing, the latest

edition was published in 2018. It is organized around six Professional Practices (PP):

- Policy and Program Management (PP1) Focuses on governance
- Embedding Business Continuity (PP2) Provides guidance on embedding BCM in the organization’s culture, which includes awareness and training

Although NIST SP 800-34 deals specifically with IT contingency plans, these steps are similar when creating enterprise-wide BCPs and BCM programs.

- Analysis (PP3) Addresses organizational review, risk assessment, and business impact analysis, among other topics
- Design (PP4) Focuses on identifying and selecting the right BC solutions
- Implementation (PP5) Addresses what should go into the BC plan
- Validation (PP6) Covers exercising, maintaining, and reviewing the program

DRI International Institute’s Professional Practices for Business Continuity Management Best practices and framework to allow for BCM processes, which are broken down into the following sections:

- Program Initiation and Management
- Risk Assessment
- Business Impact Analysis
- Business Continuity Strategies
- Incident Response
- Plan Development and Implementation
- Awareness and Training Programs
- Business Continuity Plan Exercise, Assessment, and Maintenance
- Crisis Communications
- Coordination with External Agencies

Why are there so many sets of best practices and which is the best for your organization?

If your organization is part of the U.S. government or a government contracting organization, then you need to comply with the NIST standards. If your organization is in Europe or your organization does business with other organizations in Europe, then you might need to follow the European Union Agency for Cybersecurity (ENISA) requirements. While we are not listing all of them here, there are other country-based BCM standards that your organization might need to comply with if it is residing in or does business in one of those specific countries. If your organization needs to get ISO certified, then ISO/IEC 27031 and ISO 22301 could be the standards to follow. While the first of these is focused on IT, the second is broader in scope and addresses the needs of the entire organization.

Making BCM Part of the Enterprise Security Program

As we already explained, every organization should have security policies, procedures, standards, and guidelines. People who are new to information security commonly think that this is one pile of documentation that addresses all issues pertaining to security, but it is more complicated than that—of course.

Business continuity planning ought to be fully integrated into the organization as a regular management process, just like auditing or strategic planning or other "normal" processes. Instead of being considered an outsider, BCP should be "part of the team."

An organization has no real hope of rebuilding itself and its processes after a disaster if it does not have a good understanding of how its organization works in the first place. This notion might seem absurd at first. You might think, "Well, of course an organization knows how it works." But you would be surprised at how difficult it is to fully understand an organization down to the level of detail required to rebuild it. Each individual may know and understand his or her little world within the organization, but hardly anyone at any organization can fully explain how each and every business process takes place.

Further, final responsibility for BCP should belong not to the BCP team or its leader, but to a high-level executive manager, preferably a member of the executive board. This will reinforce the image and reality of continuity planning as a function seen as vital to the organizational chiefs.

By analyzing and planning for potential disruptions to the organization, the BCP team can assist other business disciplines in their own efforts to effectively plan for and respond effectively and with resilience to emergencies. Given that the ability to respond depends on operations and management personnel throughout the organization, such capability should be developed organization-wide. It should extend throughout every location of the organization and up the employee ranks to top-tier management.

As such, the BCP program needs to be a living entity. As an organization goes through changes, so should the program, thereby ensuring it stays current, usable, and effective.

When properly integrated with change management processes, the program stands a much better chance of being continually updated and improved upon. Business continuity is a foundational piece of an effective security program and is critical to ensuring relevance in time of need.

A very important question to ask when first developing a BCP is why it is being developed. This may seem silly and the answer may at first appear obvious, but that is not always the case. You might think that the reason to have these plans is to deal with an unexpected disaster and to get people back to their tasks as quickly and as safely as possible, but the full story is often a bit different. Why are most companies in business? To make money and be profitable. If these are usually the main goals of businesses, then any BCP needs to be developed to help achieve and, more importantly, maintain these goals. The main reason to develop these plans in the first place is to reduce the risk of financial loss by improving the company's ability to recover and restore operations. This encompasses the goals of mitigating the effects of the disaster.

Not all organizations are businesses that exist to make profits. Government agencies, military units, nonprofit organizations, and the like exist to provide some type of protection or service to a nation or society. Whereas a company must create its BCP to ensure that revenue continues to come in so that the company can stay in business,

other types of organizations must create their BCPs to make sure they can still carry out their critical tasks. Although the focus and business drivers of the organizations and companies may differ, their BCPs often have similar constructs—which is to get their critical processes up and running.

Protecting what is most important to a company is rather difficult if what is most important is not first identified. Senior management is usually involved with this step because it has a point of view that extends beyond each functional manager’s focus area of responsibility. Senior management has the visibility needed to establish the scope of the plan. The company’s BCP should be focused on the company’s critical mission and business functions. And, conversely, the BCP must support the organization’s overall strategy. The functions must have priorities set upon them to indicate which is most crucial to a company’s survival. The scope of the BCP is defined by which of these functions are considered important enough to warrant the investment of resources required for BC.

As stated previously, for many companies, financial operations are most critical. As an example, an automotive company would be affected far more seriously if its credit and loan services were unavailable for a day than if, say, an assembly line went down for a day, since credit and loan services are where it generates the biggest revenues. For other organizations, customer service might be the most critical area to ensure that order processing is not negatively affected. For example, if a company makes heart pacemakers and its physician services department is unavailable at a time when an operating room surgeon needs to contact it because of a complication, the results could be disastrous for the patient. The surgeon and the company would likely be sued, and the company would likely never again be able to sell another pacemaker to that surgeon, her colleagues, or perhaps even the patient’s health maintenance organization (HMO). It would be very difficult to rebuild reputation and sales after something like that happened.

Advanced planning for emergencies covers issues that were thought of and foreseen. Many other problems may arise that are not covered in the BCP; thus, flexibility in the plan is crucial. The plan is a systematic way of providing a checklist of actions that should take place right after a disaster. These actions have been thought through to help the people involved be more efficient and effective in dealing with traumatic situations.

The most critical part of establishing and maintaining a current BCP is management support. Management must be convinced of the necessity of such a plan. Therefore, a business case must be made to obtain this support. The business case may include current vulnerabilities, regulatory and legal obligations, the current status of recovery plans, and recommendations. Management is mostly concerned with cost/benefit issues, so preliminary numbers need to be gathered and potential losses estimated. A cost/benefit analysis should include shareholder, stakeholder, regulatory, and legislative impacts, as well as impacts on products, services, and personnel. The decision of how a company should recover is commonly a business decision and should always be treated as such.

Business Impact Analysis

Business continuity planning deals with uncertainty and chance. What is important to note here is that even though you cannot predict whether or when a disaster will happen,

- Maximum tolerable downtime and disruption for activities
- Operational disruption and productivity
- Financial considerations
- Regulatory responsibilities
- Reputation

The committee will not truly understand all business processes, the steps that must take place, or the resources and supplies these processes require. So the committee must gather this information from the people who do know—department managers and specific employees throughout the organization. The committee starts by identifying the people who will be part of the BIA data-gathering sessions. The committee needs to identify how it will collect the data from the selected employees, be it through surveys, interviews, or workshops. Next, the team needs to collect the information by actually conducting surveys, interviews, and workshops. Data points obtained as part of the information gathering will be used later during analysis. It is important that the team members ask about how different tasks—whether processes, transactions, or services, along with any relevant dependencies—get accomplished within the organization. The team should build process flow diagrams, which will be used throughout the BIA and plan development stages.

Upon completion of the data collection phase, the BCP committee needs to conduct a BIA to establish which processes, devices, or operational activities are critical. If a system stands on its own, doesn’t affect other systems, and is of low criticality, then it can be classified as a tier-two or tier-three recovery step. This means these resources will not be dealt with during the recovery stages until the most critical (tier one) resources are up and running. This analysis can be completed using a standard risk assessment as illustrated in Figure 2-9.

Risk Assessment

To achieve success, the organization should systematically plan and execute a formal BCP-related risk assessment. The assessment fully takes into account the organization’s

that doesn’t mean you can’t plan for it. Just because we are not planning for an earthquake to hit us tomorrow morning at 10 ▯.▯. doesn’t mean we can’t plan the activities required to successfully survive when an earthquake (or a similar disaster) does hit. The point of making these plans is to try to think of all the possible disasters that could take place, estimate the potential damage and loss, categorize and prioritize the potential disasters, and develop viable alternatives in case those events do actually happen.

A business impact analysis (BIA) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function’s criticality level. But how do we determine a classification scheme based on criticality levels?

The BCP committee must identify the threats to the organization and map them to the following characteristics:

Figure 2-9
Risk assessment
process

Risk analysis
(including business
impact analysis)

Monitor and review

Risk identification
Risk management

Communication and consultation

Establish the content

Risk evaluation

Risk treatment

tolerance for continuity risks. The risk assessment also makes use of the data in the BIA to supply a consistent estimate of exposure.

As indicators of success, the risk assessment should identify, evaluate, and record all relevant items, which may include

- Vulnerabilities for all of the organization’s most time-sensitive resources and activities
- Threats and hazards to the organization’s most urgent resources and activities
- Measures that cut the possibility, length, or effect of a disruption on critical services and products
- Single points of failure; that is, concentrations of risk that threaten business continuity
- Continuity risks from concentrations of critical skills or critical shortages of skills
- Continuity risks due to outsourced vendors and suppliers
- Continuity risks that the BCP program has accepted, that are handled elsewhere, or that the BCP program does not address

Risk Assessment Evaluation and Process

In a BCP setting, a risk assessment looks at the impact and likelihood of various threats that could trigger a business disruption. The tools, techniques, and methods of risk assessment include determining threats, assessing probabilities, tabulating threats, and analyzing costs and benefits.

The end goals of a business continuity–focused risk assessment include

The risk assessment is assumed to take the form of the equation Risk = Threat × Impact × Probability. However, the BIA adds the dimension of time to this equation. In other words, risk mitigation measures should be geared toward those things that might most rapidly disrupt critical business processes and commercial activities.

The main parts of a risk assessment are

- Review the existing strategies for risk management
- Construct a numerical scoring system for probabilities and impacts
- Make use of a numerical score to gauge the effect of the threat
- Estimate the probability of each threat
- Weigh each threat through the scoring system
- Calculate the risk by combining the scores of likelihood and impact of each threat
- Get the organization’s sponsor to sign off on these risk priorities
- Weigh appropriate measures
- Make sure that planned measures that alleviate risk do not heighten other risks
- Present the assessment’s findings to executive management

Threats can be man-made, natural, or technical. A man-made threat may be an arsonist, a terrorist, or a simple mistake that can have serious outcomes. Natural threats may be tornadoes, floods, hurricanes, or earthquakes. Technical threats may be data corruption, loss of power, device failure, or loss of a data communications line. It is important to identify all possible threats and estimate the probability of them happening. Some issues may not immediately come to mind when developing these plans, such as an employee strike, vandals, disgruntled employees, or hackers, but they do need to be identified. These issues are often best addressed in a group with scenario-based exercises. This ensures that if a threat becomes reality, the plan includes the ramifications on all business tasks, departments, and critical operations. The more issues that are thought of and planned for, the better prepared an organization will be if and when these events take place.

- Identifying and documenting single points of failure
- Making a prioritized list of threats to the particular business processes of the organization
- Putting together information for developing a management strategy for risk control and for developing action plans for addressing risks
- Documenting acceptance of identified risks, or documenting acknowledgment of risks that will not be addressed

The BCP committee needs to step through scenarios in which the following problems result:

- Equipment malfunction or unavailable equipment

- Unavailable utilities (HVAC, power, communications lines)
- Facility becomes unavailable
- Critical personnel become unavailable
- Vendor and service providers become unavailable
- Software and/or data corruption

The specific scenarios and damage types can vary from organization to organization.

Assigning Values to Assets

Qualitative and quantitative impact information should be gathered and then properly analyzed and interpreted. The goal is to see exactly how an organization will be affected by different threats. The effects can be economical, operational, or both. Upon completion of the data analysis, it should be reviewed with the most knowledgeable people within the organization to ensure that the findings are appropriate and that it describes the real risks and impacts the organization faces. This will help flush out any additional data points not originally obtained and will give a fuller understanding of all the possible business impacts.

Loss criteria must be applied to the individual threats that were identified. The criteria may include the following:

- Loss in reputation and public confidence
- Loss of competitive advantages

BIA Steps

The more detailed and granular steps of a BIA are outlined here:

1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the organization’s critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.

We cover each of these steps in this chapter.

- Increase in operational expenses
- Violations of contract agreements
- Violations of legal and regulatory requirements
- Delayed-income costs
- Loss in revenue

• Loss in productivity

These costs can be direct or indirect and must be properly accounted for.

For instance, if the BCP team is looking at the threat of a terrorist bombing, it is important to identify which business function most likely would be targeted, how all business functions could be affected, and how each bulleted item in the loss criteria would be directly or indirectly involved. The timeliness of the recovery can be critical for business processes and the company’s survival. For example, it may be acceptable to have the customer-support functionality out of commission for two days, whereas five days may leave the company in financial ruin.

After identifying the critical functions, it is necessary to find out exactly what is required for these individual business processes to take place. The resources that are required for the identified business processes are not necessarily just computer systems, but may include personnel, procedures, tasks, supplies, and vendor support. It must be understood that if one or more of these support mechanisms is not available, the critical function may be doomed. The team must determine what type of effect unavailable resources and systems will have on these critical functions.

The BIA identifies which of the organization’s critical systems are needed for survival and estimates the outage time that can be tolerated by the organization as a result of various unfortunate events. The outage time that can be endured by an organization is referred to as the maximum tolerable downtime (MTD) or maximum tolerable period of disruption (MTPD), which is illustrated in Figure 2-10.

Figure 2-10
Maximum
tolerable
downtime

Irreparable
losses

Point at which the impact
becomes unacceptable
Serious but
survivable
losses

No loss
MTD

Time

The following are some MTD estimates that an organization may use. Note that these are sample estimates that will vary from organization to organization and from business unit to business unit.

- Nonessential 30 days
- Normal 7 days
- Important 72 hours
- Urgent 24 hours
- Critical Minutes to hours

Each business function and asset should be placed in one of these categories, depending upon how long the organization can survive without it. These estimates will help the organization determine what backup solutions are necessary to ensure the availability of these resources. The shorter the MTD, the higher priority of recovery for the function in question. Thus, the items classified as Urgent should be addressed before those classified as Normal.

For example, if being without a T1 communication line for three hours would cost the company $130,000, the T1 line could be considered Critical, and thus the company should put in a backup T1 line from a different carrier. If a server going down and being unavailable for ten days will only cost the company $250 in revenue, this would fall into the Normal category, and thus the company may not need to have a fully redundant server waiting to be swapped out. Instead, the company may choose to count on its vendor’s SLA, which may promise to have it back online in eight days.

Sometimes the MTD will depend in large measure on the type of organization in question. For instance, a call center—a vital link to current and prospective clients—will have a short MTD, perhaps measured in minutes instead of weeks. A common solution is to split up the calls through multiple call centers placed in differing locales. If one call center is knocked out of service, the other one can temporarily pick up the load. Manufacturing can be handled in various ways. Examples include subcontracting the making of products to an outside vendor, manufacturing at multiple sites, and warehousing an extra supply of products to fill gaps in supply in case of disruptions to normal manufacturing.

The BCP team must try to think of all possible events that might occur that could turn out to be detrimental to an organization. The BCP team also must understand it cannot possibly contemplate all events, and thus protection may not be available for every scenario introduced. Being properly prepared specifically for a flood, earthquake, terrorist attack, or lightning strike is not as important as being properly prepared to respond to anything that damages or disrupts critical business functions.

All of the previously mentioned disasters could cause these results, but so could a meteor strike, a tornado, or a wing falling off a plane passing overhead. So the moral of the story is to be prepared for the loss of any or all business resources, instead of focusing on the events that could cause the loss.

Identify Critical IT Resources

Input from users, business process owners, application owners, and other associated groups

Critical Business Process
1. Payroll processing
2. Time and attendance reporting
3. Time and attendance verification
4. Time and attendance approval

Critical Resources
- LAN server
- WAN access
- E-mail
- Mainframe access
- E-mail server

Identify Disruption Impacts and Allowable Outage Times
Process: 2. Time and attendance reporting
Max. allowable outage: 8 hours
Impact
- Delay in time-sheet processing
- Inability to perform payroll operations
- Delay in payroll processing

Critical Resources

- LAN server
- WAN access
- E-mail
- Mainframe access
- E-mail server

Develop Recovery Priorities

Resources

- LAN server
- WAN access
- E-mail
- Mainframe access
- E-mail server

Recovery Priority

High
Medium
Low
High
High

EXAM TIP A BIA is performed at the beginning of business continuity planning to identify the areas that would suffer the greatest financial or operational loss in the event of a disaster or disruption. It identifies the organization’s critical systems needed for survival and estimates the outage time that can be tolerated by the organization as a result of a disaster or disruption.

Chapter Review

We took a very detailed look at the way in which we manage risk to our information systems. We know that no system is truly secure, so our job is to find the most likely and the most dangerous threat actions so that we can address them first. The process of quantifying losses and their probabilities of occurring is at the heart of risk assessments.

Armed with that information, we are able to make good decisions in terms of controls, processes, and costs. Our approach is focused not solely on the human adversary but also on any source of loss to our organizations. Most importantly, we use this information to devise ways in which to ensure we can continue business operations in the face of any reasonable threat.

Quick Review

- Risk management is the process of identifying and assessing risk, reducing it to an acceptable level, and ensuring it remains at that level.
- An information systems risk management (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.
- A threat is a potential cause of an unwanted incident, which may result in harm to a system or organization.
- Four risk assessment methodologies with which you should be familiar are NIST SP 800-30; Facilitated Risk Analysis Process (FRAP); Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE); and Failure Modes and Effect Analysis (FMEA).
- Failure Modes and Effect Analysis (FMEA) is a method for determining functions, identifying functional failures, and assessing the causes of failure and their effects through a structured process.
- A fault tree analysis is a useful approach to detect failures that can take place within complex environments and systems.
- A quantitative risk analysis attempts to assign monetary values to components within the analysis.
- A purely quantitative risk analysis is not possible because qualitative items cannot be quantified with precision.
- Qualitative risk analysis uses judgment and intuition instead of numbers.
- Qualitative risk analysis involves people with the requisite experience and education evaluating threat scenarios and rating the probability, potential loss, and severity of each threat based on their personal experience.
- Single loss expectancy × frequency per year = annualized loss expectancy (SLE × ARO = ALE)

- The main goals of risk analysis are the following: identify assets and assign values to them, identify vulnerabilities and threats, quantify the impact of potential threats, and provide an economic balance between the impact of the risk and the cost of the safeguards.
- Capturing the degree of uncertainty when carrying out a risk analysis is important, because it indicates the level of confidence the team and management should have in the resulting figures.
- Automated risk analysis tools reduce the amount of manual work involved in the analysis. They can be used to estimate future expected losses and calculate the benefits of different security measures.
- The risk management team should include individuals from different departments within the organization, not just technical personnel.
- Risk can be transferred, avoided, reduced, or accepted.

- Threats × vulnerability × asset value = total risk.
- (Threats × vulnerability × asset value) × controls gap = residual risk.
- When choosing the right safeguard to reduce a specific risk, the cost, functionality, and effectiveness must be evaluated and a cost/benefit analysis performed.
- There are three main categories of controls: administrative, technical, and physical.
- Controls can also be grouped by types, depending on their intended purpose, as preventive, detective, corrective, deterrent, recovery, and compensating.
- A control assessment is an evaluation of one or more controls to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome.
- Security control verification answers the question “did we implement the control right?” while validation answers the question “did we implement the right control?”
- Risk monitoring is the ongoing process of adding new risks, reevaluating existing ones, removing moot ones, and continuously assessing the effectiveness of your controls at mitigating all risks to tolerable levels.
- Change management processes deal with monitoring changes to your environment and dealing with the risks they could introduce.
- Continuous improvement is the practice of identifying opportunities, mitigating threats, improving quality, and reducing waste as an ongoing effort. It is the hallmark of mature and effective organizations.
- A supply chain is a sequence of suppliers involved in delivering some product.
- Business continuity management (BCM) is the overarching approach to managing all aspects of BCP and DRP.
- A business continuity plan (BCP) contains strategy documents that provide detailed procedures that ensure critical business functions are maintained and that help minimize losses of life, operations, and systems.

- A BCP provides procedures for emergency responses, extended backup operations, and post-disaster recovery.
- A BCP should have an enterprise-wide reach, with each individual organizational unit having its own detailed continuity and contingency plans.
- A BCP needs to prioritize critical applications and provide a sequence for efficient recovery.
- A BCP requires senior executive management support for initiating the plan and final approval.
- BCPs can quickly become outdated due to personnel turnover, reorganizations, and undocumented changes.
- Executives may be held liable if proper BCPs are not developed and used.
- Threats can be natural, man-made, or technical.
- The business impact analysis (BIA) is one of the most important first steps in the planning development. Qualitative and quantitative data on the business impact of

a disaster need to be gathered, analyzed, interpreted, and presented to management.

- Executive commitment and support are the most critical elements in developing the BCP.
- A business case must be presented to gain executive support. This is done by explaining regulatory and legal requirements, exposing vulnerabilities, and providing solutions.
- Plans should be prepared by the people who will actually carry them out.
- The planning group should comprise representatives from all departments or organizational units.
- The BCP team should identify the individuals who will interact with external players, such as the reporters, shareholders, customers, and civic officials. Response to the disaster should be done quickly and honestly, and should be consistent with any other organizational response.

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. When is it acceptable to not take action on an identified risk?
A. Never. Good security addresses and reduces all risks.
B. When political issues prevent this type of risk from being addressed.
C. When the necessary countermeasure is complex.
D. When the cost of the countermeasure outweighs the value of the asset and

potential loss.

A. Risk analysis
B. Cost/benefit analysis
C. ALE results
D. Identifying the vulnerabilities and threats causing the risk

3. Which best describes the purpose of the ALE calculation?
A. Quantifies the security level of the environment
B. Estimates the loss possible for a countermeasure
C. Quantifies the cost/benefit result
D. Estimates the loss potential of a threat in a span of a year

4. How do you calculate residual risk?
A. Threats × risks × asset value
B. (Threats × asset value × vulnerability) × risks
C. SLE × frequency = ALE
D. (Threats × vulnerability × asset value) × controls gap

5. Why should the team that will perform and review the risk analysis

information
be made up of people in different departments?

A. To make sure the process is fair and that no one is left out.

B. It shouldn’t. It should be a small group brought in from outside the organization because otherwise the analysis is biased and unusable.

C. Because people in different departments understand the risks of their department. Thus, it ensures the data going into the analysis is as close to reality as possible.

D. Because the people in the different departments are the ones causing the risks, so they should be the ones held accountable.

6. Which best describes a quantitative risk analysis?

A. A scenario-based analysis to research different security threats

B. A method used to apply severity levels to potential loss, probability of loss, and risks

C. A method that assigns monetary values to components in the risk assessment

D. A method that is based on gut feelings and opinions

7. Why is a truly quantitative risk analysis not possible to achieve?

A. It is possible, which is why it is used.

B. It assigns severity levels. Thus, it is hard to translate into monetary values.

C. It is dealing with purely quantitative elements.

D. Quantitative measures must be applied to qualitative elements.

2. Which is the most valuable technique when determining if a specific security control should be implemented?

Use the following scenario to answer Questions 9–11. A company has an e-commerce website that carries out 60 percent of its annual revenue. Under the current circumstances, the annualized loss expectancy for a website against the threat of attack is $92,000. After implementing a new application-layer firewall, the new ALE would be $30,000. The firewall costs $65,000 per year to implement and maintain.

8. How much does the firewall save the company in loss expenses?

A. $62,000

B. $3,000

C. $65,000

D. $30,000

9. What is the value of the firewall to the company?

A. $62,000

B. $3,000

C. –$62,000

D. –$3,000

10. Which of the following describes the company’s approach to risk management?
A. Risk transference
B. Risk avoidance
C. Risk acceptance
D. Risk mitigation

Use the following scenario to answer Questions 11–13. A small remote office for a company is valued at $800,000. It is estimated, based on historical data, that a fire is likely to occur once every ten years at a facility in this area. It is estimated that such a fire would destroy 60 percent of the facility under the current circumstances and with the current detective and preventive controls in place.
11. What is the single loss expectancy (SLE) for the facility suffering from a fire?
A. $80,000
B. $480,000
C. $320,000
D. 60%

12. What is the annualized rate of occurrence (ARO)?
A. 1
B. 10
C. .1
D. .01

13. What is the annualized loss expectancy (ALE)?
B. $32,000
C. $48,000
D. .6

14. Which of the following is not one of the three key areas for risk monitoring?
A. Threat
B. Effectiveness
C. Change
D. Compliance

15. What is one of the first steps in developing a business continuity plan?
A. Identify a backup solution.
B. Perform a simulation test.
C. Perform a business impact analysis.
D. Develop a business resumption plan.

Answers
1. D. Organizations may decide to live with specific risks they are faced with if the cost of trying to protect themselves would be greater than the potential loss if

the threat were to become real. Countermeasures are usually complex to a degree, and there are almost always political issues surrounding different risks, but these are not reasons to not implement a countermeasure.

2. B. Although the other answers may seem correct, B is the best answer here. This is because a risk analysis is performed to identify risks and come up with suggested countermeasures. The annualized loss expectancy (ALE) tells the organization how much it could lose if a specific threat became real. The ALE value will go into the cost/benefit analysis, but the ALE does not address the cost of the countermeasure and the benefit of a countermeasure. All the data captured in answers A, C, and D is inserted into a cost/benefit analysis.

3. D. The ALE calculation estimates the potential loss that can affect one asset from a specific threat within a one-year time span. This value is used to figure out the amount of money that should be earmarked to protect this asset from this threat.

4. D. The equation is more conceptual than practical. It is hard to assign a number to an individual vulnerability or threat. This equation enables you to look at the potential loss of a specific asset, as well as the controls gap (what the specific countermeasure cannot protect against). What remains is the residual risk, which is what is left over after a countermeasure is implemented.

A. $480,000

5. C. An analysis is only as good as the data that goes into it. Data pertaining to risks the organization faces should be extracted from the people who understand best the business functions and environment of the organization. Each department understands its own threats and resources, and may have possible solutions to specific threats that affect its part of the organization.

6. C. A quantitative risk analysis assigns monetary values and percentages to the different components within the assessment. A qualitative analysis uses opinions of individuals and a rating system to gauge the severity level of different threats and the benefits of specific countermeasures.

7. D. During a risk analysis, the team is trying to properly predict the future and all the risks that future may bring. It is somewhat of a subjective exercise and requires educated guessing. It is very hard to properly predict that a flood will take place once in ten years and cost a company up to $40,000 in damages, but this is what a quantitative analysis tries to accomplish.

8. A. $62,000 is the correct answer. The firewall reduced the annualized loss expectancy

(ALE) from $92,000 to $30,000 for a savings of $62,000. The formula for ALE is single loss expectancy × annualized rate of occurrence = ALE. Subtracting the ALE value after the firewall is implemented from the value before it was implemented results in the potential loss savings this type of control provides.

9. D. –$3,000 is the correct answer. The firewall saves $62,000, but costs $65,000 per year. 62,000 – 65,000 = –3,000. The firewall actually costs the company more than the original expected loss, and thus the value to the company is a negative number. The formula for this calculation is (ALE before the control is implemented) – (ALE after the control is implemented) – (annual cost of control) = value of control.

10. D. Risk mitigation involves employing controls in an attempt to reduce either the likelihood or damage associated with an incident, or both. The four ways of dealing with risk are accept, avoid, transfer, and mitigate (reduce). A firewall is a countermeasure installed to reduce the risk of a threat.

11. B. $480,000 is the correct answer. The formula for single loss expectancy (SLE) is asset value × exposure factor (EF) = SLE. In this situation the formula would work out as asset value ($800,000) × exposure factor (60%) = $480,000. This means that the company has a potential loss value of $480,000 pertaining to this one asset (facility) and this one threat type (fire).

12. C. The annualized rate occurrence (ARO) is the frequency that a threat will most likely occur within a 12-month period. It is a value used in the ALE formula, which is SLE × ARO = ALE.

13. C. $48,000 is the correct answer. The annualized loss expectancy formula (SLE × ARO = ALE) is used to calculate the loss potential for one asset experiencing one threat in a 12-month period. The resulting ALE value helps to determine the amount that can reasonably be spent in the protection of that asset.
In this situation, the company should not spend over $48,000 on protecting this

asset from the threat of fire. ALE values help organizations rank the severity level of the risks they face so they know which ones to deal with first and how much to spend on each.

14. A. Risk monitoring activities should be focused on three key areas: effectiveness, change, and compliance. Changes to the threat landscape should be incorporated directly into the first two, and indirectly into compliance monitoring.

15. C. A business impact analysis includes identifying critical systems and functions of an organization and interviewing representatives from each department. Once management’s support is solidified, a BIA needs to be performed to identify the threats the company faces and the potential costs of these threats.

This page intentionally left blank

CHAPTER

Compliance

This chapter presents the following:

- Regulations, laws, and crimes involving computers
- Intellectual property
- Data breaches
- Compliance requirements
- Investigations

If you think compliance is expensive, try noncompliance.
—Paul McNulty

Rules, formal or otherwise, are essential for prosperity in any context. This is particularly true when it comes to cybersecurity. Even if our adversaries don’t follow the rules (and clearly they don’t), we must understand the rules that apply to us and follow them carefully. In this chapter, we discuss the various laws and regulations that deal with computer information systems. We can’t really address each piece of legislation around the world, since that would take multiple books longer than this one. However, we will offer as examples some of the most impactful laws and regulations affecting multinational enterprises. These include laws and regulations applicable to cybercrimes, privacy, and intellectual property, among others. The point of this chapter is not to turn you into a cyberlaw expert, but to make you aware of some of the topics about which you should have conversations with your legal counsel and compliance colleagues as you develop and mature your cybersecurity program.

Laws and Regulations

Before we get into the details of what you, as a cybersecurity leader, are required to do, let’s start by reviewing some foundational concepts about what laws and regulations are, exploring how they vary around the world, and then putting them into a holistic context.

Law is a system of rules created by either a government or a society, recognized as binding by that group, and enforced by some specific authority. Laws apply equally to everyone in the country or society. It is important to keep in mind that laws are not always written down and may be customary, as discussed shortly. Regulations, by contrast, are written rules dealing with specific details or procedures, issued by an executive body and having the force of law. Regulations apply only to the specific entities that fall under the authority of the agency that issues them. So, while any U.S.-based organization is subject to a U.S. law called the Computer Fraud and Abuse Act (CFAA), only U.S. organizations that deal with data concerning persons in the European Union (EU) would also be subject to the General Data Protection Regulation (GDPR).

Types of Legal Systems

Your organization may be subject to laws and regulations from multiple jurisdictions. As just mentioned, if your organization is based in the United States but handles data of citizens of the EU, your organization is subject to both the CFAA and the GDPR. It is important to keep in mind that different countries can have very different legal systems. Your legal department will figure out jurisdictions and applicability, but you need to be aware of what this disparity of legal systems means to your cybersecurity program. To this end, it is helpful to become familiar with the major legal systems you may come across. In this section, we cover the core components of the various legal systems and what differentiates them.

Civil (Code) Law System

- System of law used in continental European countries such as France and Spain.
- Different legal system from the common law system used in the United Kingdom and United States.
- Civil law system is rule-based law, not precedent-based.
- For the most part, a civil law system is focused on codified law—or written laws.
- The history of the civil law system dates to the sixth century when the Byzantine emperor Justinian codified the laws of Rome.
- Civil legal systems should not be confused with the civil (or tort) laws found in the United States.
- The civil legal system was established by states or nations for self-regulation; thus, the civil law system can be divided into subdivisions, such as French civil law, German civil law, and so on.
- It is the most widespread legal system in the world and the most common legal system in Europe.

- Under the civil legal system, lower courts are not compelled to follow the decisions made by higher courts.

Common Law System

- Developed in England.
- Based on previous interpretations of laws:
- In the past, judges would walk throughout the country enforcing laws and settling disputes.

Criminal Law System

- Based on common law, statutory law, or a combination of both.
- Addresses behavior that is considered harmful to society.
- Punishment usually involves a loss of freedom, such as incarceration, or monetary fines.
- Responsibility is on the prosecution to prove guilt beyond a reasonable doubt (innocent until proven guilty).

Civil/Tort Law System

- Offshoot of criminal law.
- Under civil law, the defendant owes a legal duty to the victim. In other words, the defendant is obligated to conform to a particular standard of conduct, usually set by what a “reasonable person of ordinary prudence” would do to prevent foreseeable injury to the victim.
- The defendant’s breach of that duty causes injury to the victim; usually physical or financial.
- Categories of civil law:
- Intentional Examples include assault, intentional infliction of emotional distress, or false imprisonment.
- Wrongs against property An example is nuisance against landowner.
- Wrongs against a person Examples include car accidents, dog bites, and a slip and fall.
- Negligence An example is wrongful death.
- Nuisance An example is trespassing.

- The judges did not have a written set of laws, so they based their laws on custom and precedent.
- In the 12th century, the king of England (Henry II) imposed a unified legal system that was “common” to the entire country.
- Reflects the community’s morals and expectations.
- Led to the creation of barristers, or lawyers, who actively participate in the litigation process through the presentation of evidence and arguments.
- Today, the common law system uses judges and juries of peers. If the jury trial is waived, the judge decides the facts.

- Typical systems consist of a higher court, several intermediate appellate courts, and many local trial courts. Precedent flows down through this system. Tradition also allows for “magistrate’s courts,” which address administrative decisions.
- The common law system is broken down into criminal, civil/tort, and administrative.

- Dignitary wrongs Include invasion of privacy and civil rights violations.
- Economic wrongs Examples include patent, copyright, and trademark infringement.
- Strict liability Examples include a failure to warn of risks and defects in product manufacturing or design.

Administrative (Regulatory) Law System

- Laws and legal principles created by administrative agencies to address a number of areas, including international trade, manufacturing, environment, and immigration.

Customary Law System

- Deals mainly with personal conduct and patterns of behavior.
- Based on traditions and customs of the region.
- Emerged when cooperation of individuals became necessary as communities merged.
- Not many countries work under a purely customary law system, but instead use a mixed system where customary law is an integrated component. (Codified civil law systems emerged from customary law.)
- Mainly used in regions of the world that have mixed legal systems (for example, China and India).
- Restitution is commonly in the form of a monetary fine or service.

Religious Law System

- Based on religious beliefs of the region.
- In Islamic countries, the law is based on the rules of the Koran.
- The law, however, is different in every Islamic country.
- Jurists and clerics have a high degree of authority.
- Covers all aspects of human life, but commonly divided into
- Responsibilities and obligations to others.
- Religious duties.
- Knowledge and rules as revealed by God, which define and govern human affairs.
- Rather than create laws, lawmakers and scholars attempt to discover the truth of law.
- Law, in the religious sense, also includes codes of ethics and morality, which are upheld and required by God. For example, Hindu law, Sharia (Islamic law), Halakha (Jewish law), and so on.

Mixed Law System

- Two or more legal systems are used together and apply cumulatively or interactively.

Civil law

Common law

Mixed systems

Religious law

Asia
Europe

North
America
Caribbean
Central
America

Africa

Middle
East
Southeast
Asia

South
America
Oceania

Common Law Revisited

These different legal systems are certainly complex, and while you are not expected to be a lawyer to pass the CISSP exam, having a high-level understanding of the different types (civil, common, customary, religious, mixed) is important. The exam will dig more into the specifics of the common law legal system and its components. Under the common law legal system, civil law deals with wrongs against individuals or organizations that result in damages or loss. This is referred to as tort law. Examples include trespassing, battery, negligence, and product liability. A successful civil lawsuit against a defendant would result in financial restitution and/or community service instead of a jail sentence. When someone sues another person in civil court, the jury decides upon liability instead of innocence or guilt. If the jury determines the defendant is liable for the act, then the jury decides upon the compensatory and/or punitive damages of the case.

Criminal law is used when an individual’s conduct violates the government laws, which have been developed to protect the public. Jail sentences are commonly the punishment for criminal law cases that result in conviction, whereas in civil law cases the punishment is usually an amount of money that the liable individual must pay the victim. For example, in the O.J. Simpson case, the defendant was first tried and found

- Most often mixed law systems consist of civil and common law.
- A combination of systems is used as a result of more or less clearly defined fields of application.
- Civil law may apply to certain types of crimes, while religious law may apply to other types within the same region.
- Examples of mixed law systems include those in Holland, Canada, and South Africa.

not guilty in the criminal law case, but then was found liable in the civil law case. This seeming contradiction can happen because the burden of proof is lower in civil cases than in criminal cases.

EXAM TIP Civil law generally is derived from common law (case law), cases are initiated by private parties, and the defendant is found liable or not liable for damages. Criminal law typically is statutory, cases are initiated by government prosecutors, and the defendant is found guilty or not guilty.

Administrative/regulatory law deals with regulatory standards that regulate performance and conduct. Government agencies create these standards, which are usually applied to companies and individuals within those specific industries. Some examples of administrative laws could be that every building used for business must have a fire detection and suppression system, must have clearly visible exit signs, and cannot have blocked doors, in case of a fire. Companies that produce and package food and drug products are regulated by many standards so that the public is protected and aware of their actions. If an administrative law case determines that a company did not abide by specific regulatory standards, officials in the company could even be held accountable.

For example, if a company makes tires that shred after a couple of years of use because the company doesn’t comply with manufacturing safety standards, the officers in that company could be liable under administrative, civil, or even criminal law if they were aware of the issue but chose to ignore it to keep profits up.

Cybercrimes and Data Breaches

So far, we’ve discussed laws and regulations only in a general way to provide a bit of context. Let’s now dive into the laws and regulations that are most relevant to our roles as cybersecurity leaders. Computer crime laws (sometimes collectively referred to as cyberlaw) around the world deal with some of the core issues: unauthorized access, modification or destruction of assets, disclosure of sensitive information, and the use of malware (malicious software).

Although we usually only think of the victims and their systems that were attacked during a crime, laws have been created to combat three categories of crimes. A computerassisted crime is where a computer was used as a tool to help carry out a crime. A computertargeted crime concerns incidents where a computer was the victim of an attack crafted to harm it (and its owners) specifically. The last type of crime is where a computer is not necessarily the attacker or the target, but just happened to be involved when a crime was carried out. This category is referred to as computer is incidental.

Some examples of computer-assisted crimes are

- Exploiting financial systems to conduct fraud
- Stealing military and intelligence material from government computer systems
- Conducting industrial espionage by attacking competitors and gathering confidential business data

Some examples of computer-targeted crimes include

- Distributed denial-of-service (DDoS) attacks
- Stealing passwords or other sensitive data from servers
- Installing cryptominers to mine cryptocurrency on someone else’s computers
- Conducting a ransomware attack

NOTE The main issues addressed in computer crime laws are unauthorized modification, disclosure, destruction, or access and inserting malicious programming code.

Some confusion typically exists between the two categories—computer-assisted crimes and computer-targeted crimes—because intuitively it would seem any attack would fall into both of these categories. One system is carrying out the attacking, while the other system is being attacked. The difference is that in computer-assisted crimes, the computer is only being used as a tool to carry out a traditional type of crime. Without computers, people still steal, cause destruction, protest against organizations (for example, companies that carry out experiments upon animals), obtain competitor information, and go to war. So these crimes would take place anyway; the computer is simply one of the tools available to the attacker. As such, it helps that threat actor become more efficient at carrying out a crime.

Computer-assisted crimes are usually covered by regular criminal laws in that they are not always considered a “computer crime.” One way to look at it is that a computertargeted crime could not take place without a computer, whereas a computer-assisted crime could. Thus, a computer-targeted crime is one that did not, and could not, exist before use of computers became common. In other words, in the good old days, you could not carry out a buffer overflow on your neighbor or install malware on your enemy’s system. These crimes require that computers be involved.

If a crime falls into the “computer is incidental” category, this means a computer just happened to be involved in some secondary manner, but its involvement is still significant. For example, if you have a friend who works for a company that runs the state lottery and he gives you a printout of the next three winning numbers and you type them into your computer, your computer is just the storage place. You could have just kept the piece of paper and not put the data in a computer. Another example is child pornography. The actual crime is obtaining and sharing child pornography pictures or graphics. The pictures could be stored on a file server or they could be kept in a physical file in someone’s desk. So if a crime falls within this category, the computer is not attacking another computer and a computer is not being attacked, but the computer is still used in some significant manner.

- Carrying out information warfare activities by leveraging compromised influential accounts
- Engaging in hacktivism, which is protesting a government’s or organization’s activities by attacking its systems and/or defacing its website

Because computing devices are everywhere in modern society, computers are incidental to most crimes today. In a fatal car crash, the police may seize the drivers' mobile devices to look for evidence that either driver was texting at the time of the accident. In a domestic assault case, investigators may seek a court order to obtain the contents of the home's virtual assistant, such as Amazon Alexa, because it may contain recorded evidence of the crime.

You may say, "So what? A crime is a crime. Why break it down into these types of categories?" The reason these types of categories are created is to allow current laws to apply to these types of crimes, even though they are in the digital world. Let's say someone is on your computer just looking around, not causing any damage, but she should not be there. Should legislators have to create a new law stating, "Thou shall not browse around in someone else's computer," or should law enforcement and the courts just apply the already created trespassing law? What if a hacker got into a trafficcontrol system and made all of the traffic lights turn green at the exact same time? Should legislators go through the hassle of creating a new law for this type of activity, or should law enforcement and the courts use the already created (and understood) manslaughter and murder laws? Remember, a crime is a crime, and a computer is just a new tool to carry out traditional criminal activities.

Now, this in no way means countries can just depend upon the laws on the books and that every computer crime can be countered by an existing law. Many countries have had to come up with new laws that deal specifically with different types of computer crimes.

For example, the following are just some of the laws that have been created or modified in the United States to cover the various types of computer crimes:

- 18 USC 1029: Fraud and Related Activity in Connection with Access Devices
- 18 USC 1030: Fraud and Related Activity in Connection with Computers
- 18 USC 2510 et seq.: Wire and Electronic Communications Interception and Interception of Oral Communications
- 18 USC 2701 et seq.: Stored Wire and Electronic Communications and Transactional Records Access
- Digital Millennium Copyright Act
- Cyber Security Enhancement Act of 2002

EXAM TIP You do not need to know these laws for the CISSP exam; they are just examples.

Complexities in Cybercrime

Since we have a bunch of laws to get the digital bad guys, this means we have this whole cybercrime thing under control, right? Alas, cybercrimes have only increased over the years and will not stop anytime soon. Several contributing factors explain why these activities have not been properly stopped or even curbed. These include issues related

Attack

Attack

Attack

Trust Relationship

Trust Relationship

Small Business

Figure 3-1 A typical island-hopping attack

Regional Supplier

Multinational
Corporation

to proper attribution of the attacks, the necessary level of protection for networks, and successful prosecution once an attacker is captured.

Many attackers are never caught because they spoof their addresses and identities and use methods to cover their digital footsteps. Many attackers break into networks, take whatever resources they were after, and clean the logs that tracked their movements and activities. Because of this, many organizations do not even know their systems have been violated. Even if an attacker's activities are detected, it does not usually lead to the true identity of the individual, though it does alert the organization that a specific vulnerability was exploited.

Attackers commonly hop through several systems before attacking their victim so that tracking down the attackers will be more difficult. This is exemplified by a threat actor approach known as an island-hopping attack, which is when the attacker compromises an easier target that is somehow connected to the ultimate one. For instance, consider a major corporation like the one depicted on the right side of Figure 3-1. It has robust cybersecurity and relies on a regional supplier for certain widgets. Since logistics are oftentimes automated, these two companies have trusted channels of communication between them so their computers can talk to each other about when more widgets might be needed and where. The supplier, in turn, relies on a small company that produces special screws for the widgets. This screw manufacturer employs just a couple of people working out of the owner’s garage and is a trivial target for an attacker. So, rather than target the major corporation directly, a cybercriminal could attack the screw manufacturer’s unsecured computers, use them to gain a foothold in the supplier, and then use that company’s trusted relationship with the well-defended target to ultimately get into its systems. This particular type of island-hopping attack is also known as a supply-chain attack because it exploits trust mechanisms inherent in supply chains.

Many companies that are victims of an attack usually just want to ensure that the vulnerability the attacker exploited is fixed, instead of spending the time and money to go after and prosecute the attacker. This is a huge contributing factor as to why cybercriminals get away with their activities. Some regulated organizations—for instance, financial institutions—by law, must report breaches. However, most organizations do not have to report breaches or computer crimes. No company wants its dirty laundry out in the open for everyone to see. The customer base will lose confidence, as will

the shareholders and investors. We do not actually have true computer crime statistics because most are not reported.

Although regulations, laws, and attacks help make senior management more aware of security issues, when their company ends up in the headlines with reports of how they lost control of over 100,000 credit card numbers, security suddenly becomes very important to them.

NOTE Even though some institutions must, by law, report security breaches and crimes, that does not mean they all follow this law. Some of these institutions, just like many other organizations, often simply fix the vulnerability and sweep the details of the attack under the carpet.

The Evolution of Attacks

Perpetrators of cybercrime have evolved from bored teenagers with too much time on their hands to organized crime rings with very defined targets and goals. In the early 1990s, hackers were mainly made up of people who just enjoyed the thrill of hacking. It was seen as a challenging game without any real intent of harm. Hackers used to take down large websites (e.g., Yahoo!, MSN, Excite) so their activities made the headlines and they won bragging rights among their fellow hackers. Back then, virus writers created viruses that simply replicated or carried out some benign activity, instead of the more malicious actions they could have carried out. Unfortunately, today, these trends have taken on more sinister objectives as the Internet has become a place of business. This evolution is what drove the creation of the antivirus (now antimalware) industry.

Three powerful forces converged in the mid to late 1990s to catapult cybercrime forward. First, with the explosive growth in the use of the Internet, computers became much more lucrative targets for criminals. Second, there was an abundance of computer experts who had lost their livelihoods with the end of the Soviet Union. Some of these bright minds turned to cybercrime as a way to survive the tough times in which they found themselves. Finally, with increased demand for computing systems, many software developers were rushing to be first to market, all but ignoring the security (or lack thereof) of their products and creating fertile ground for remote attacks from all over the world. These forces resulted in the emergence of a new breed of cybercriminal possessing knowledge and skills that quickly overwhelmed many defenders. As the impact of the increased threat was realized, organizations around the world started paying more attention to security in a desperate bid to stop their cybercrime losses.

In the early 2000s, there was a shift from cybercriminals working by themselves to the formation of organized cybercrime gangs. This change dramatically improved the capabilities of these threat actors and allowed them to go after targets that, by then, were very well defended. This shift also led to the creation of vast, persistent attack infrastructures on a global scale. After cybercriminals attacked and exploited computers, they maintained a presence for use in support of later attacks. Nowadays, these exploited targets are known as malicious bots, and they are usually organized into botnets. These botnets can be used to carry out DDoS attacks, transfer spam or pornography, or do whatever the attacker commands the bot software to do. Figure 3-2 shows the many uses cybercriminals have for compromised computers.

Spam Zombie

Phishing Site
Malware Download Site

DDoS Extortion Zombie
Web Server

Bot Activity

Click Fraud Zombie
Anonymization Proxy
CAPTCHA Solving Zombie

Child Pornography Server
Spam Site
HACKED PC

eBay/Paypal Fake Auctions

Webmail Spam
Stranded Abroad Advance Scams
Harvesting E-mail Contacts

E-mail Attacks

Account
Credentials

Harvesting Associated Accounts

Online Gaming Credentials
Website FTP Credentials
Skype/VoIP Credentials
Client-Side Encryption Certificates

Access to Corporate E-mail

Bank Account Data

Online Gaming Characters
Online Gaming Goods/Currency

Virtual Goods

Financial
Credentials

Operating System License Key

Mutual Fund/401(k) Account

Facebook
Twitter
Linkedln
Google+

Credit Card Data
Stock Trading Account

PC Game License Keys

Fake Antivirus
Reputation Hijacking

Hostage Attacks

Ransomware
E-mail Account Ransom
Webcam Image Extortion

Figure 3-2 Malicious uses for a compromised computer (Source: www.krebsonsecurity.com)

EXAM TIP You may see the term script kiddies on the exam (or elsewhere). It refers to hackers who do not have the requisite skills to carry out specific attacks without the tools provided on the Internet or through friends.

A recent development in organized cybercrime is the emergence of so-called Hacking as a Service (HaaS), which is a play on cloud computing services such as Software as a Service (SaaS). HaaS represents the commercialization of hacking skills, providing access to tools, target lists, credentials, hackers for hire, and even customer support. In the last couple of years, there has been a significant increase in the number of marketplaces in which HaaS is available.
Many times hackers are just scanning systems looking for a vulnerable running service or sending out malicious links in e-mails to unsuspecting victims. They are just looking for any way to get into any network. This would be the shotgun approach to network attacks. Another, more dangerous, attacker has you in the proverbial crosshairs

and is determined to identify your weakest point and exploit it. As an analogy, the thief that goes around rattling door knobs to find one that is not locked is not half as dangerous as the one who will watch you day in and day out to learn your activity patterns, where you work, what type of car you drive, and who your family is and patiently wait for your most vulnerable moment to ensure a successful and devastating attack.

We call this second type of attacker an advanced persistent threat (APT). This is a military term that has been around for ages, but since the digital world is effectively a

Warez/Piracy Server

battleground, this term is more relevant each and every day. How an APT differs from the plain old vanilla attacker is that the APT is commonly a group of attackers, not just one hacker, that combine their knowledge and abilities to carry out whatever exploit will get them into the environment they are seeking. The APT is very focused and motivated to aggressively and successfully penetrate a network with various different attack methods and then clandestinely hide its presence while achieving a well-developed, multilevel foothold in the environment.

The “advanced” aspect of the term APT pertains to the expansive knowledge, capabilities, and skill base of the APT. The “persistent” component has to do with the fact that the group of attackers is not in a hurry to launch an attack quickly, but will wait for the most beneficial moment and attack vector to ensure that its activities go unnoticed. This is what we refer to as a “low-and-slow” attack. This type of attack is coordinated by human involvement, rather than just a virus type of threat that goes through automated steps to inject its payload. The APT has specific objectives and goals and is commonly highly organized and well funded, which makes it the biggest threat of all.

APTs commonly use custom-developed malicious code that is built specifically for its target, has multiple ways of hiding itself once it infiltrates the environment, may be able to polymorph itself in replication capabilities, and has several different “anchors” to make it hard to eradicate even if it is discovered. Once the code is installed, it commonly sets up a covert back channel (as regular bots do) so that it can be remotely controlled by the group of attackers. The remote control functionality allows the attackers to traverse the network with the goal of gaining continuous access to critical assets.

APT infiltrations are usually very hard to detect with host-based solutions because the attackers put the code through a barrage of tests against the most up-to-date detection applications on the market. A common way to detect these types of threats is through network traffic changes. For example, changes in DNS queries coming out of your network could indicate that an APT has breached your environment and is using DNS tunneling to establish command and control over the compromised hosts. The APT will likely have multiple control servers and techniques to communicate so that if one connection gets detected and removed, the APT still has an active channel to use. The APT may implement encrypted tunnels over HTTPS so that its data that is in transmission cannot be inspected. Figure 3-3 illustrates the common steps and results of APT activity.

The ways of getting into a network are basically endless (exploit a web service, induce users to open e-mail links and attachments, gain access through remote maintenance accounts, exploit operating systems and application vulnerabilities, compromise connections from home users, etc.). Each of these vulnerabilities has its own fixes (patches, proper configuration, awareness, proper credential practices, encryption, etc.).

It is not only these fixes that need to be put in place; we need to move to a more effective situational awareness model. We need to have better capabilities of knowing what is happening throughout our network in near to real time so that our defenses can react quickly and precisely.

The landscape continues to evolve, and the lines between threat actors are sometimes blurry. We already mentioned the difficulty in attributing an attack to a specific individual so that criminal charges may be filed. Something that makes this even harder is the practice among some governments of collaborating with criminal groups in their countries.

Figure 3-3 Gaining access into an environment and extracting sensitive data

Common Internet Crime Schemes

- Business e-mail compromise
- Business fraud
- Charity and disaster fraud
- Counterfeit prescription drugs
- Credit card fraud
- Election crimes and security
- Identity theft
- Illegal sports betting
- Nigerian letter, or “419”
- Ponzi/pyramid
- Ransomware
- Sextortion

Find out how these types of computer crimes are carried out by visiting https://www.fbi.gov/scams-and-safety/common-scams-and-crimes.

Do You Trust Your Neighbor?

Most organizations do not like to think about the fact that the enemy might be inside the organization and working internally. It is more natural to view threats as the faceless unknowns that reside on the outside of our environment. Employees have direct and privileged access to an organization’s assets, and they are commonly not as highly monitored compared to traffic that is entering the network from external entities. The combination of too much trust, direct access, and the lack of monitoring allows for a lot of internal fraud and abuse to go unnoticed.

There have been many criminal cases over the years where employees at various organizations have carried out embezzlement or have launched revenge attacks after they were fired or laid off. While it is important to have fortified walls to protect us from the outside forces that want to cause us harm, it is also important to realize that our underbelly is more vulnerable. Employees, contractors, and temporary workers who have direct access to critical resources introduce risks that need to be understood and countermeasured.

The way it works is that the government looks the other way as long as the crimes are committed in other countries. When the government needs a bit of help to obfuscate what it’s doing to another government, it enlists the help of the cybercrime gang they’ve been protecting (or at least tolerating) and tell them what to do and to whom. To the target, it looks like a cybercrime but in reality it had nation-state goals.

So while the sophistication of the attacks continues to increase, so does the danger of these attacks. Isn’t that just peachy?

Up until now, we have listed some difficulties of fighting cybercrime: the anonymity the Internet provides the attacker; attackers are organizing and carrying out more sophisticated attacks; the legal system is running to catch up with these types of crimes; and organizations are just now viewing their data as something that must be protected. All these complexities aid the bad guys, but what if we throw in the complexity of attacks taking place between different countries?

International Issues

If a hacker in Ukraine attacks a bank in France, whose legal jurisdiction is that? How do these countries work together to identify the criminal and carry out justice? Which country is required to track down the criminal? And which country should take this person to court? Well, the short answer is: it depends.

When computer crime crosses international boundaries, the complexity of such issues shoots up considerably and the chances of the criminal being brought to any court decreases. This is because different countries have different legal systems, some countries have no laws pertaining to computer crime, jurisdiction disputes may erupt, and some governments may not want to play nice with each other. For example, if someone in Iran attacked a system in Israel, do you think the Iranian government would help Israel track down the attacker? What if someone in North Korea attacked a military system in the

Data Breaches

Among the most common cybercrimes are those relating to the theft of sensitive data. In fact, it is a rare month indeed when one doesn’t read or hear about a major data breach. Information is the lifeblood of most major corporations nowadays, and threat actors know this. They have been devoting a lot of effort over the past several years to compromising and exploiting the data stores that, in many ways, are more valuable to organizations than any vault full of cash. This trend continues unabated, which makes data breaches one of the most important issues in cybersecurity today.

In a way, data breaches can be thought of as the opposite of privacy: data owners lose control of who has the ability to access their data. When an organization fails to properly protect the privacy of its customers’ data, it increases the likelihood of experiencing a data breach. It should not be surprising, therefore, that some of the same legal and regulatory issues that apply to privacy also apply to data breaches.

It is important to note that data breaches need not involve a violation of personal privacy. Indeed, some of the most publicized data breaches have had nothing to do with personally identifiable information (PII) but with intellectual property (IP). It is worth pausing to properly define the term data breach as a security event that results in the actual or potential compromise of the confidentiality or integrity of protected information by unauthorized actors. Protected information can be PII, IP, protected health information (PHI), classified information, or any other information that can cause damage to an individual or organization.

PART I

United States? Do you think these two countries would work together to find the hacker?

Maybe or maybe not—or perhaps the attack was carried out by a government agency pretending to be a cybercrime gang.

There have been efforts to standardize the different countries’ approaches to computer crimes because they happen so easily over international boundaries. Although it is very easy for an attacker in China to send packets through the Internet to a bank in Saudi Arabia, it is very difficult (because of legal systems, cultures, and politics) to motivate these governments to work together.

The Council of Europe (CoE) Convention on Cybercrime, also known as the Budapest Convention, is one example of an attempt to create a standard international response to cybercrime. In fact, it is the first international treaty seeking to address computer crimes by coordinating national laws and improving investigative techniques and international cooperation. One of the requirements of the treaty is that signatories develop national legislation outlawing a series of cybercrimes, such as hacking, computer-related fraud, and child pornography. The convention’s objectives also include the creation of a framework for establishing jurisdiction and extradition of the accused. For example, extradition can only take place when the event is a crime in both jurisdictions. As of April 2021, 68 countries around the world (not just in Europe) have signed or ratified the treaty, contributing to the global growth in effective cybercrime legislation that is internationally interoperable. According to the United Nations (UN), 79 percent of the world’s countries (that’s 154) now have cybercrime laws. All these laws vary, of course, but they may impact your own organization depending on where you do business and with whom.

Personally Identifiable Information

Personally identifiable information (PII) is data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. PII needs to be highly protected because it is commonly used in identity theft, financial crimes, and various criminal activities.

While it seems as though defining and identifying PII should be easy and straightforward, what different countries, federal governments, and state governments consider to be PII differs.

The U.S. Office of Management and Budget in its memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” defines PII as “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.” Determining what constitutes PII, then, depends on a specific risk assessment of the likelihood that the information can be used to uniquely identify an individual. This is all good and well, but doesn’t really help us recognize information that might be considered PII. Typical components are listed here:

- Full name (if not common)
- National identification number
- Home address
- IP address (in some cases)
- Vehicle registration plate number
- Driver’s license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Birthday
- Birthplace

- Genetic information

The following items are less often used because they are commonly shared by so many people, but they can fall into the PII classification and may require protection from improper disclosure:

- First or last name, if common
- Country, state, or city of residence
- Age, especially if nonspecific

As a security professional, it is important to understand which legal and regulatory requirements are triggered by data breaches. To further complicate matters, most U.S. states, as well as many other countries, have enacted distinct laws with subtle but important differences in notification stipulations. As always when dealing with legal issues, it is best to consult with an attorney. This section is simply an overview of some of the legal requirements of which you should be aware.

U.S. Laws Pertaining to Data Breaches

We've already mentioned various U.S. federal statutes dealing with cybercrimes. Despite our best efforts, there will be times when our information systems are compromised and personal information security controls are breached. Let's briefly highlight some of the laws that are most relevant to data breaches:

- California Consumer Privacy Act (CCPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HI-TECH) Act
- Gramm-Leach-Bliley Act of 1999
- Economic Espionage Act of 1996

It is worth recalling here that data breaches are not only violations of customer privacy. When a threat actor compromises a target corporation's network and exposes its intellectual property, a breach has occurred. While the other laws we have discussed in this section deal with protecting customers' PII, the Economic Espionage Act protects corporations' IP. When you think of data breaches, it is critical that you consider both PII and IP exposure.

Almost every U.S. state has enacted legislation that requires government and private entities to disclose data breaches involving PII. The most important of these is probably the California Consumer Privacy Act, which went into effect in 2020. The CCPA is perhaps the broadest and most far-reaching of U.S. state laws around PII breaches, but it is certainly not the only one. In almost every case, PII is defined by the states as the combination of first and last name with any of the following:

- Social Security number
- Driver’s license number
- Credit or debit card number with the security code or PIN

- Gender or race
- Name of the school they attend or workplace
- Grades, salary, or job position
- Criminal record

Unfortunately, that is where the commonalities end. The laws are so different that compliance with all of them is a difficult and costly issue for most corporations. In some states, simple access to files containing PII triggers a notification requirement, while in other states the organization must only notify affected parties if the breach is reasonably likely to result in illegal use of the information. Many experts believe that the CCPA will set an example for other states and may provide a template for other countries.

European Union Laws Pertaining to Data Breaches

Global organizations that move data across other country boundaries must be aware of and follow the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Since most countries have a different set of laws pertaining to the definition of private data and how it should be protected, international trade and business get more convoluted and can negatively affect the economy of nations. The OECD is an international organization that helps different governments come together and tackle the economic, social, and governance challenges of a globalized economy. Because of this, the OECD came up with guidelines for the various countries to follow so that data is properly protected and everyone follows the same type of rules.

The core principles defined by the OECD are as follows:

- Collection Limitation Principle Collection of personal data should be limited, obtained by lawful and fair means, and with the knowledge of the subject.
- Data Quality Principle Personal data should be kept complete and current and be relevant to the purposes for which it is being used.
- Purpose Specification Principle Subjects should be notified of the reason for the collection of their personal information at the time that it is collected, and organizations should only use it for that stated purpose.
- Use Limitation Principle Only with the consent of the subject or by the authority of law should personal data be disclosed, made available, or used for purposes other than those previously stated.
- Security Safeguards Principle Reasonable safeguards should be put in place to protect personal data against risks such as loss, unauthorized access, modification, and disclosure.
- Openness Principle Developments, practices, and policies regarding personal data should be openly communicated. In addition, subjects should be able to easily establish the existence and nature of personal data, its use, and the identity and usual residence of the organization in possession of that data.
- Individual Participation Principle Subjects should be able to find out whether an organization has their personal information and what that information is, to correct erroneous data, and to challenge denied requests to do so.
- Accountability Principle Organizations should be accountable for complying with measures that support the previous principles.

Although the OECD Guidelines were a great start, they were not enforceable or uniformly applied. The European Union in many cases takes individual privacy much more seriously than most other countries in the world, so in 1995 it enacted the Data Protection Directive (DPD). As a directive, it was not directly enforceable, but EU member states were required to enact laws that were consistent with it. The intent of this was to create a set of laws across the EU that controlled the way in which European organizations had to protect the personal data and privacy of EU citizens. The Safe Harbor Privacy Principles were then developed to outline how U.S.-based organizations could comply with European privacy laws. For a variety of reasons, this system of directives, laws, and principles failed to work well in practice and had to be replaced.
The General Data Protection Regulation (GDPR) was adopted by the EU in April 2016 and became enforceable in May 2018. It protects the personal data and privacy of EU citizens. The GDPR, unlike a directive such as the DPD, has the full weight of a law in all 27 member states of the EU. This means that each state does not have

to write its own version, which harmonizes data protection regulations and makes it easier for organizations to know exactly what is expected of them throughout the bloc. The catch is that these requirements are quite stringent, and violating them exposes an organization to a maximum fine of 4 percent of that organization’s global turnover. For a company like Google, that would equate to over $4 billion if they were ever shown to not be in compliance. Ouch!

The GDPR defines three relevant entities:

- Data subject The individual to whom the data pertains
- Data controller Any organization that collects data on EU residents
- Data processor Any organization that processes data for a data controller

The regulation applies if any one of the three entities is based in the EU, but it also applies if a data controller or processor has data pertaining to an EU resident. The GDPR impacts every organization that holds or uses European personal data both inside and outside of Europe. In other words, if your organization is a U.S.-based company that has never done business with the EU, but it has an EU citizen working as a summer intern, it probably has to comply with the GDPR or risk facing stiff penalties.

The GDPR set of protected types of privacy data is more inclusive than regulations and laws outside the EU. Among others, protected privacy data includes

- Name
- Address
- ID numbers

NOTE Information on the OECD Guidelines can be found at www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

- Web data (location, IP address, cookies)
- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

To ensure this data is protected, the GDPR requires that most data controllers and data processors formally designate a Data Protection Officer (DPO). DPOs are internal

compliance officers that act semi-independently to ensure that their organizations follow the letter of the regulation. While DPOs are not ultimately responsible if their organizations are not in compliance (at least according to the GDPR), in practice they are charged with monitoring compliance, advising controllers on when and how to conduct data protection impact assessments, and maintaining all required records.
Key provisions of the GDPR include

- Consent Data controllers and data processors cannot use personal data without explicit consent of the data subjects.
- Right to be informed Data controllers and data processors must inform data subjects about how their data is, will, or could be used.
- Right to restrict processing Data subjects can agree to have their data stored by a collector but disallow it to be processed.
- Right to be forgotten Data subjects can request that their personal data be permanently deleted.
- Data breaches Data controllers must report a data breach to the supervisory authority of the EU member state involved within 72 hours of becoming aware of it.

Other Nations’ Laws Pertaining to Data Breaches

As might be expected, the rest of the world is a hodgepodge of laws with varying data breach notification conditions and requirements. As of this writing, the United Nations lists at least 62 countries that have no legally mandated notification requirements whatsoever. This is concerning because unscrupulous organizations have been known to outsource their data-handling operations to countries with no data breach laws in order to circumvent the difficulties in reconciling the different country and state requirements.

The EU’s GDPR, though it has been called too restrictive and costly by some, has served as a model for other countries to implement similar legislation. For example, the two newest data protection laws, which came into full effect in 2020, are Brazil’s General Personal Data Protection Law (Lei Geral de Proteção de Dados, or LGPD) and Thailand’s Personal Data Protection Act (PDPA). Both apply to all organizations that handle the personal information of these countries’ residents, whether they are physically located within the country or not. Thailand’s PDPA further provides for jail time in particularly egregious cases.

⮝Chapter 3: Compliance

Import/Export Controls