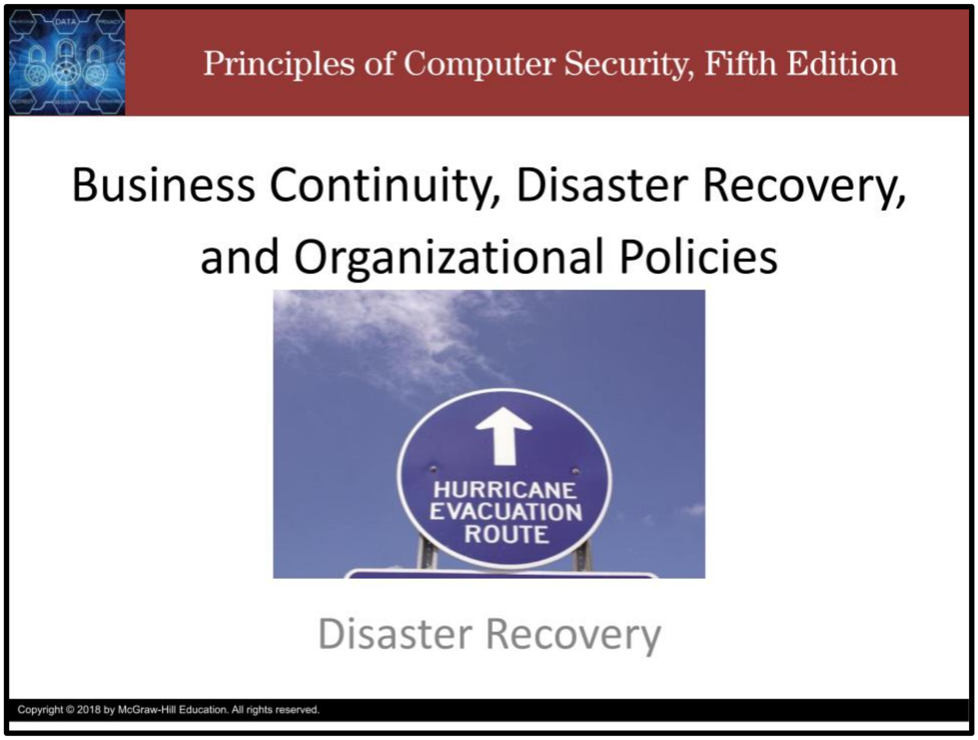
Business Continuity, Disaster Recovery, and Organizational Policies: Disaster Recovery

Slide 1



Principles of Computer Security, Fifth Edition

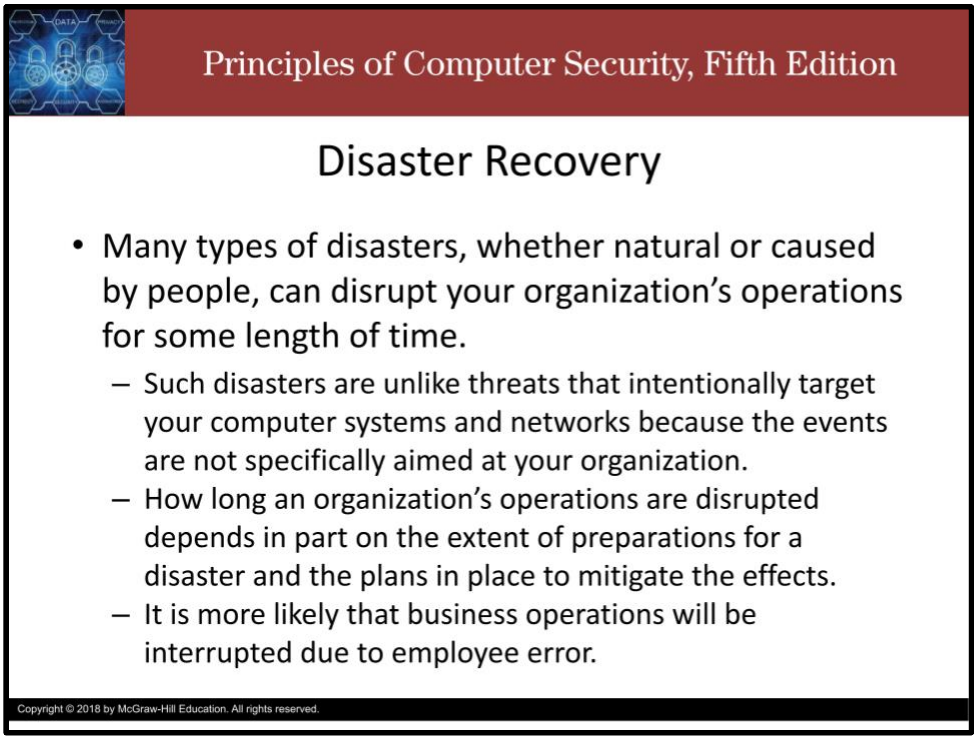
Business Continuity, Disaster Recovery, and Organizational Policies

HURRICANE EVACUATION ROUTE

Disaster Recovery

Howdy! In this video, we discuss disaster recovery.

Slide 2



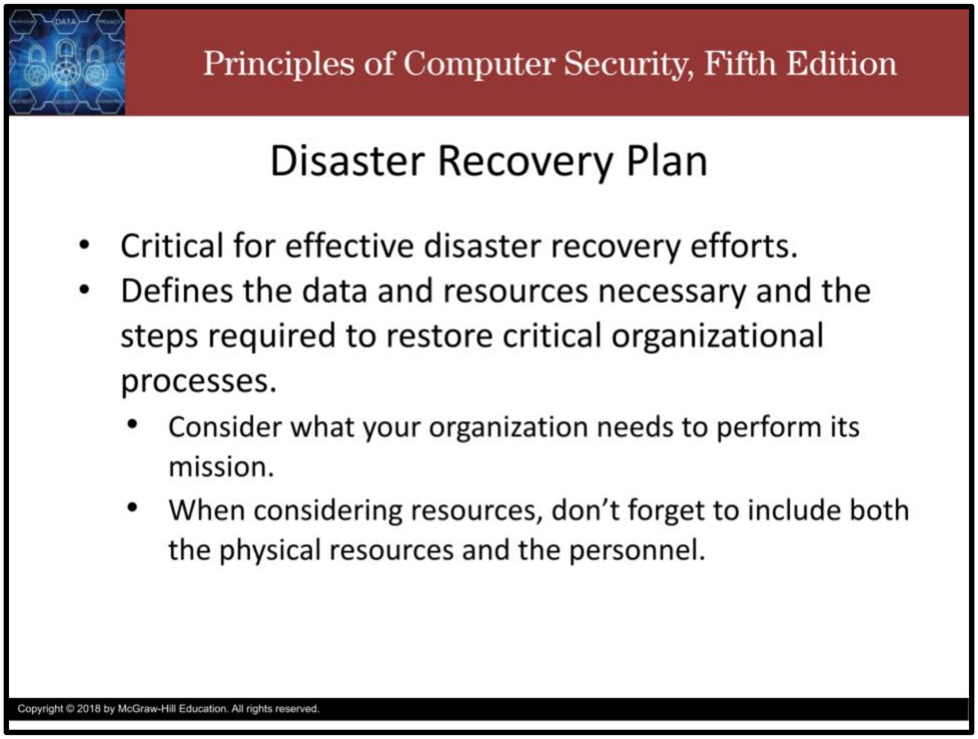
Principles of Computer Security, Fifth Edition

Disaster Recovery

- Many types of disasters, whether natural or caused by people, can disrupt your organization’s operations for some length of time.
  - Such disasters are unlike threats that intentionally target your computer systems and networks because the events are not specifically aimed at your organization.
  - How long an organization’s operations are disrupted depends in part on the extent of preparations for a disaster and the plans in place to mitigate the effects.
  - It is more likely that business operations will be interrupted due to employee error.

Many types of disasters, whether natural or caused by people, can disrupt your organization’s operations for some length of time. Such disasters are unlike threats that intentionally target your computer systems and networks, such as industrial espionage, hacking, attacks from disgruntled employees, and insider threats, because the events that cause the disruption are not specifically aimed at your organization. Although both disasters and intentional threats must be considered important in planning for disaster recovery, the purpose of this video is to focus on recovering from disasters. How long your organization’s operations are disrupted depends in part on how prepared it is for a disaster and what plans are in place to mitigate the effects of a disaster. It is more likely that business operations will be interrupted due to employee error (such as accidental corruption of a database or unplugging a system to plug in a vacuum cleaner—an event that has occurred at more than one organization). A good disaster recovery plan will prepare your organization for any type of organizational disruption.

Slide 3



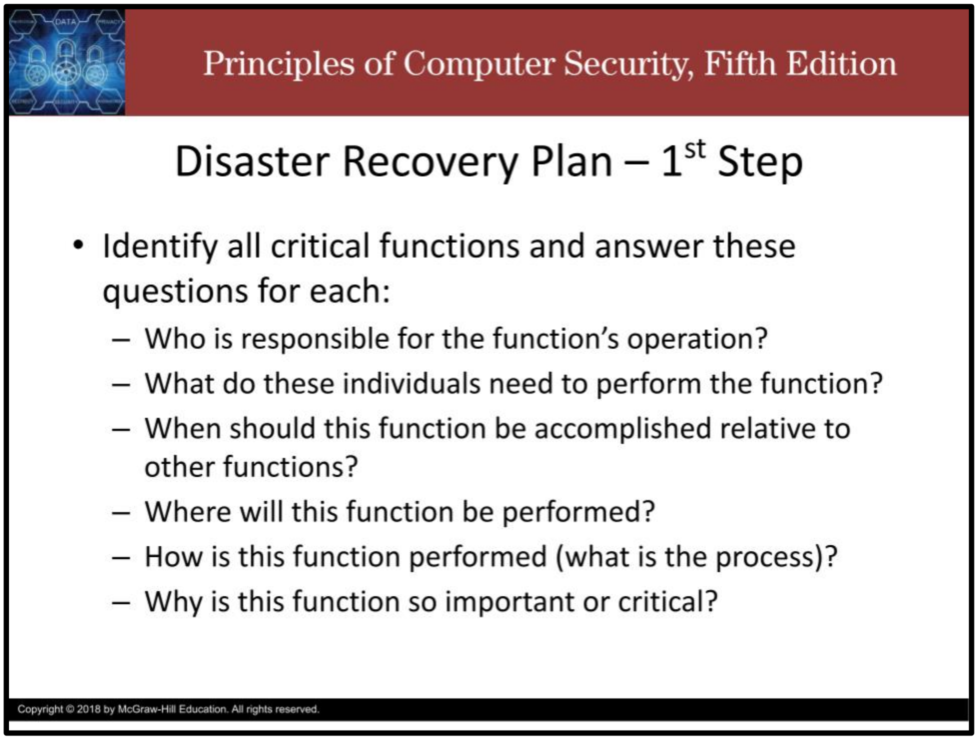
Principles of Computer Security, Fifth Edition

Disaster Recovery Plan

- Critical for effective disaster recovery efforts.
- Defines the data and resources necessary and the steps required to restore critical organizational processes.
  - Consider what your organization needs to perform its mission.
  - When considering resources, don’t forget to include both the physical resources and the personnel.

No matter what event you are worried about—whether natural or not, targeted at your organization or not—you can make preparations to lessen the impact on your organization and the length of time that your organization will be out of operation. A **disaster recovery plan (DRP)** is critical for effective disaster recovery efforts. A DRP defines the data and resources necessary and the steps required to restore critical organizational processes. Consider what your organization needs to perform its mission. This information provides the beginning of a DRP, since it tells you what needs to be quickly restored. When considering resources, don’t forget to include both the physical resources (such as computer hardware and software) and the personnel (the people who know how to run the systems that process your critical data).

Slide 4



Principles of Computer Security, Fifth Edition

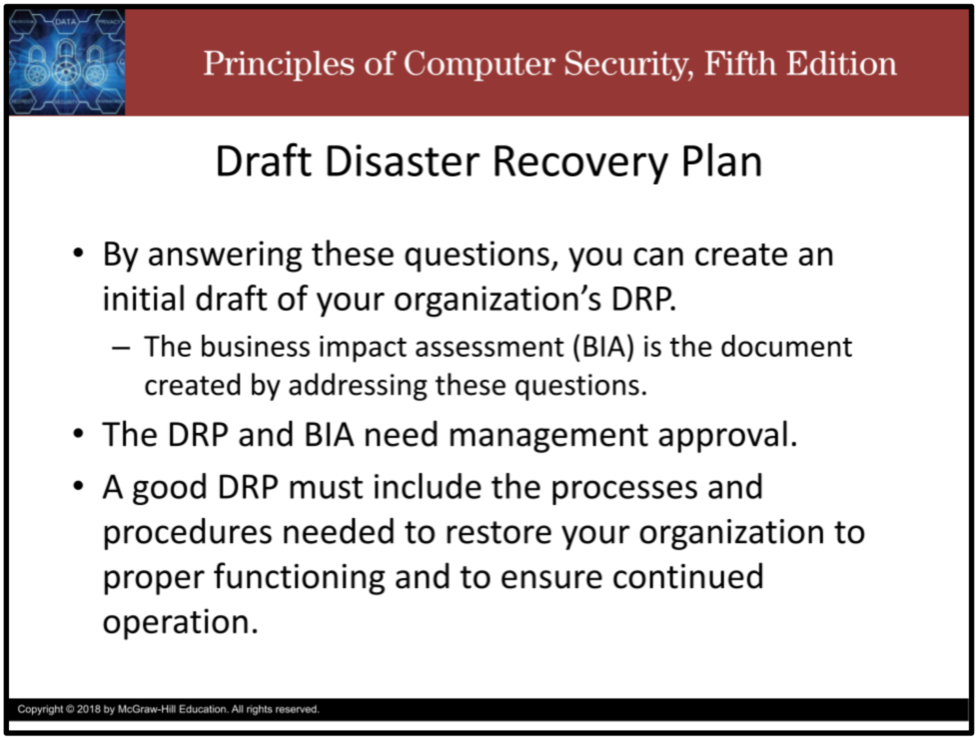
Disaster Recovery Plan – 1st Step

- Identify all critical functions and answer these questions for each:
  - Who is responsible for the function's operation?
  - What do these individuals need to perform the function?
  - When should this function be accomplished relative to other functions?
  - Where will this function be performed?
  - How is this function performed (what is the process)?
  - Why is this function so important or critical?

To begin creating your DRP, first identify all critical functions for your organization, and then answer the following questions for each of these critical functions:

Who is responsible for the operation of this function?
What do these individuals need to perform the function?
When should this function be accomplished relative to other functions?
Where will this function be performed?
How is this function performed (what is the process)?
Why is this function so important or critical to the organization?

Slide 5



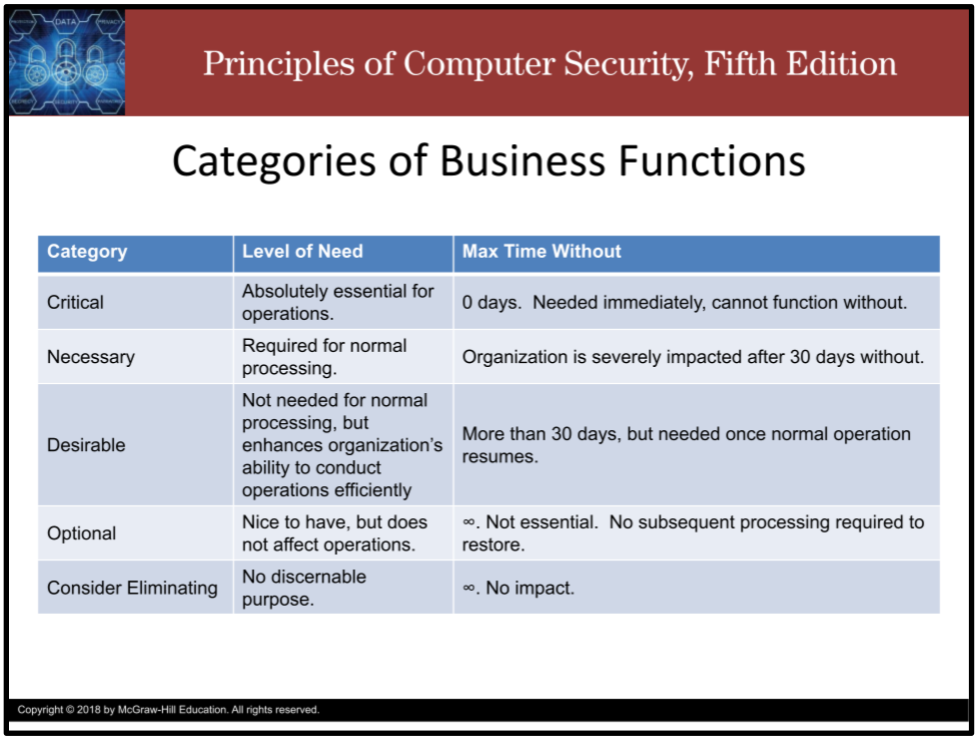
Principles of Computer Security, Fifth Edition

Draft Disaster Recovery Plan

- By answering these questions, you can create an initial draft of your organization’s DRP.
  - The business impact assessment (BIA) is the document created by addressing these questions.
- The DRP and BIA need management approval.
- A good DRP must include the processes and procedures needed to restore your organization to proper functioning and to ensure continued operation.

By answering these questions, you can create an initial draft of your organization’s DRP. The name often used to describe the document created by addressing these questions is a business impact assessment (BIA). Both the DRP and the BIA need to be approved by management and it is essential that they buy into the plan—otherwise your efforts will more than likely fail. As they say: “Those who fail to plan, plan to fail”. A good DRP must include the processes and procedures needed to restore your organization to proper functioning and to ensure continued operation. What specific steps will be required to restore operations? These processes should be documented and, where possible and feasible, reviewed and exercised on a periodic basis. Having a plan with step-by-step procedures that nobody knows how to follow does nothing to ensure the continued operation of the organization. Exercising your DRP and processes before a disaster occurs provides you with the opportunity to discover flaws or weaknesses in the plan when there is still time to modify and correct them. It also provides an opportunity for key figures in the plan to practice what they will be expected to accomplish.

Slide 6



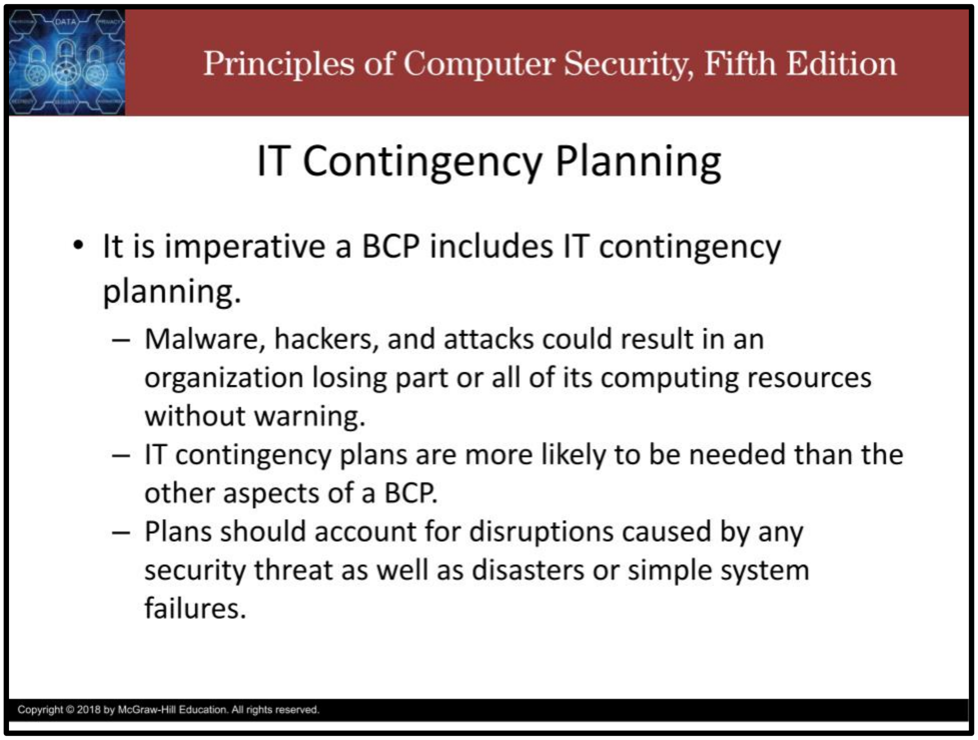
Principles of Computer Security, Fifth Edition

Categories of Business Functions

Category	Level of Need	Max Time Without
Critical	Absolutely essential for operations.	0 days. Needed immediately, cannot function without.
Necessary	Required for normal processing.	Organization is severely impacted after 30 days without.
Desirable	Not needed for normal processing, but enhances organization's ability to conduct operations efficiently	More than 30 days, but needed once normal operation resumes.
Optional	Nice to have, but does not affect operations.	∞. Not essential. No subsequent processing required to restore.
Consider Eliminating	No discernable purpose.	∞. No impact.

In developing your DRP, you may find it useful to categorize the various functions your organization performs. This categorization is based on how critical or important the function is to your business operation and how long your organization can last without the function. Those functions that are the most critical should be restored first, and your DRP should reflect this. The DRP is crucial part of the business continuity plan, which will be used to ensure that your operations continue in the face of whatever event has occurred that has caused a disruption in operations. If a disaster has occurred and has destroyed all or part of your facility, the DRP portion of the business continuity plan will address the building or acquisition of a new facility. The DRP can also include details related to the long-term recovery of the organization. However you view these two plans, an organization that is not able to quickly restore business functions after an operational interruption is an organization that will most likely suffer an unrecoverable loss and may cease to exist.

Slide 7



Principles of Computer Security, Fifth Edition

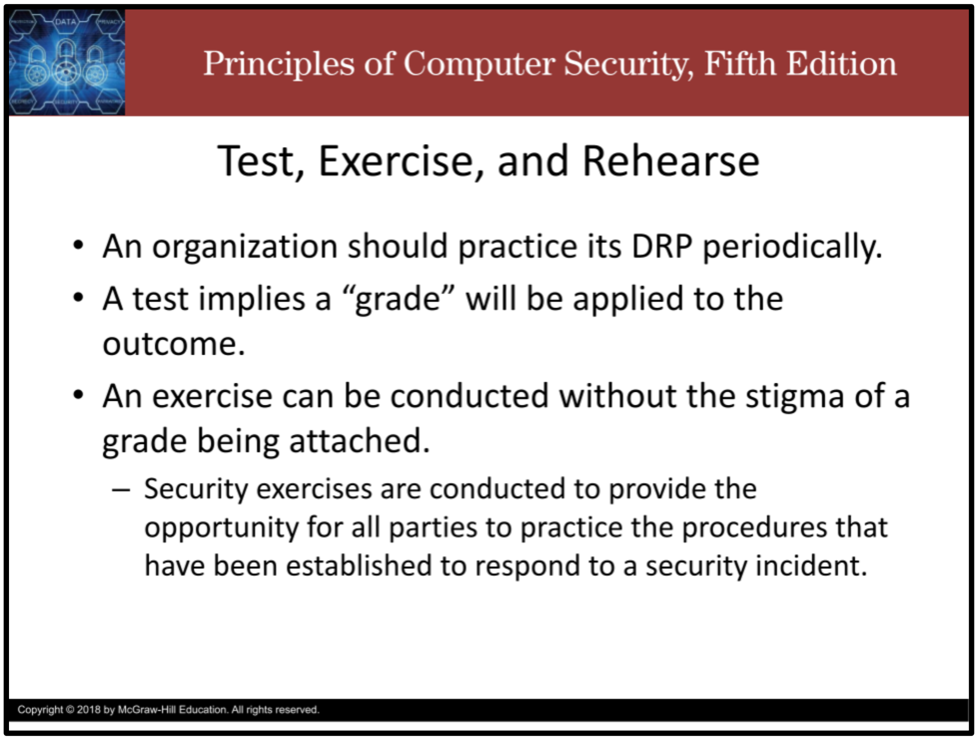
IT Contingency Planning

- It is imperative a BCP includes IT contingency planning.
  - Malware, hackers, and attacks could result in an organization losing part or all of its computing resources without warning.
  - IT contingency plans are more likely to be needed than the other aspects of a BCP.
  - Plans should account for disruptions caused by any security threat as well as disasters or simple system failures.

Some of the most important parts of any organization are the IT processes and assets. Without computers and networks, most organizations could not operate. As a result, it is imperative that a business continuity plan include IT contingency planning. Due to the nature of the Internet and the threats that come from it, an organization’s IT assets will likely face some level of disruption before the organization suffers from a disruption due to a natural disaster.

Events such as viruses, worms, computer intruders, and denial-of-service attacks could result in an organization losing part or all of its computing resources without warning.
Consequently, the IT contingency plans are more likely to be needed than the other aspects of a business continuity plan.
These plans should account for disruptions caused by any security threat as well as disasters or system failures.

Slide 8



Principles of Computer Security, Fifth Edition

Test, Exercise, and Rehearse

- An organization should practice its DRP periodically.
- A test implies a “grade” will be applied to the outcome.
- An exercise can be conducted without the stigma of a grade being attached.
  - Security exercises are conducted to provide the opportunity for all parties to practice the procedures that have been established to respond to a security incident.

An organization should practice its DRP periodically. The time to find out whether it has flaws is not when an actual event occurs, when recovery of data and information means the continued existence of the organization.

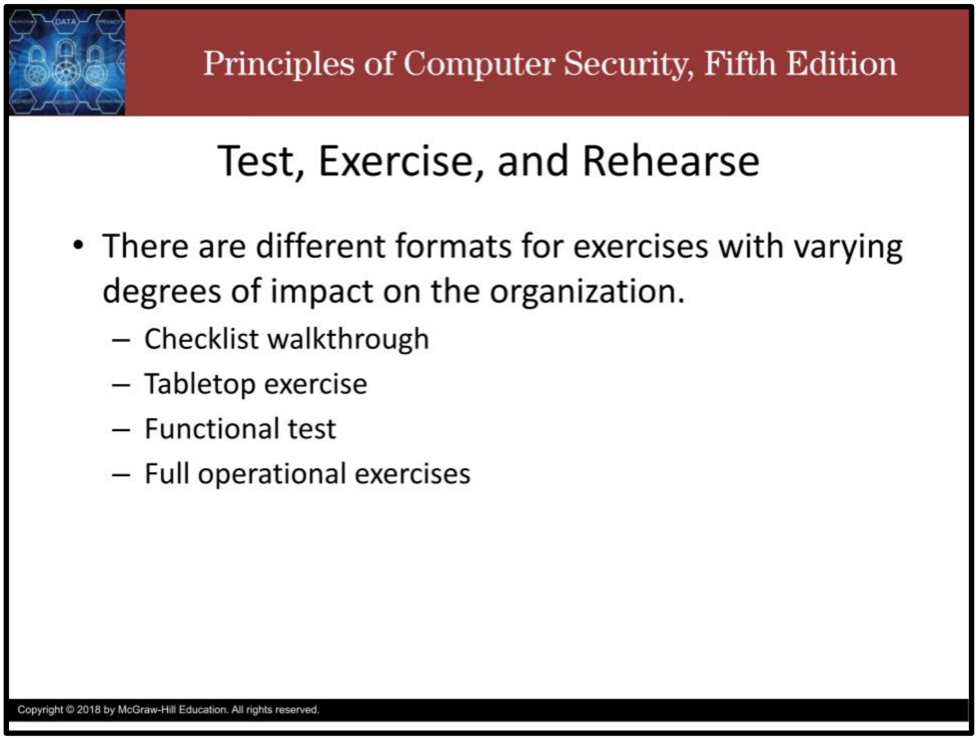
The DRP should be tested to ensure that it is sufficient and that all key individuals know their role in the specific plan. The security plan determines if the organization’s plan and the individuals involved perform as they should during a simulated security incident.

A test implies a “grade” will be applied to the outcome. Did the organization’s plan and the individuals involved perform as they should? Was the organization able to recover and continue to operate within the predefined tolerances set by management? If the answer is no, then during the follow-up evaluation of the exercise, the failures should be identified and addressed. Was it simply a matter of untrained or uninformed individuals, or was there a technological failure that necessitates a change in hardware, software, and procedures?

While a test implies a “grade,” an exercise can be conducted without the stigma of a grade being attached. Security exercises are conducted to provide the opportunity for all parties to practice the procedures that have been established to respond to a security incident. It is important to perform as many of the recovery functions as possible, without impacting ongoing operations, to ensure that the procedures and technology will work in a real incident.

You may want to periodically rehearse portions of the recovery plan, particularly those aspects that either are potentially more disruptive to actual operations or require more frequent practice because of their importance or degree of difficulty.

Slide 9



Principles of Computer Security, Fifth Edition

Test, Exercise, and Rehearse

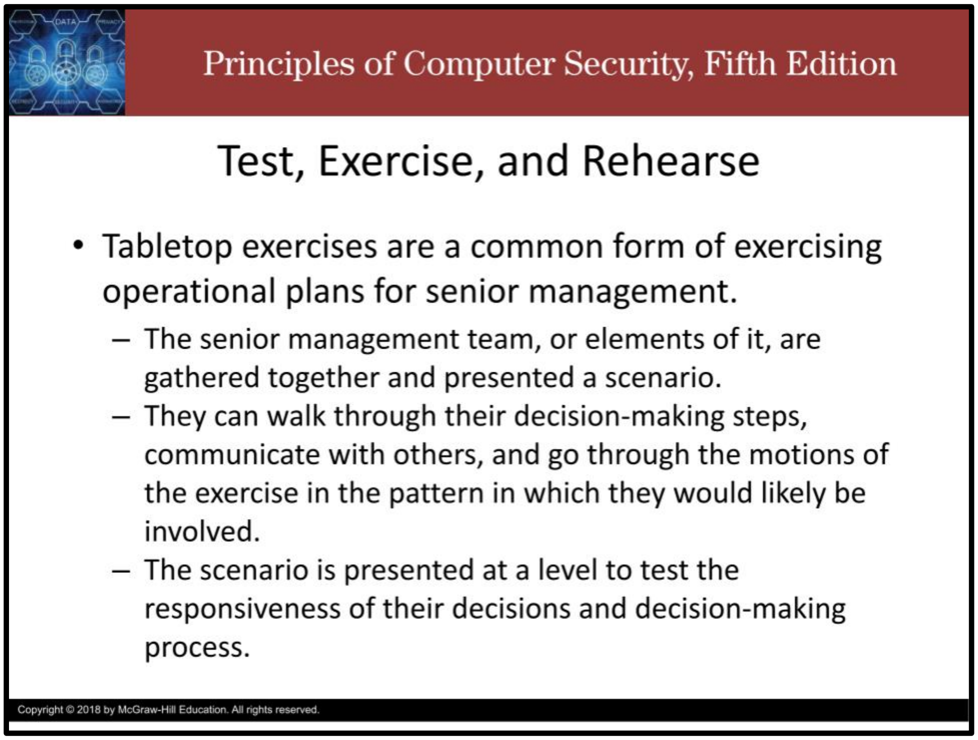
- There are different formats for exercises with varying degrees of impact on the organization.
  - Checklist walkthrough
  - Tabletop exercise
  - Functional test
  - Full operational exercises

Additionally, there are different formats for exercises with varying degrees of impact on the organization. The most basic is a checklist walkthrough in which individuals go through a recovery checklist to ensure that they understand what to do should the plan be invoked and confirm that all necessary equipment (hardware and software) is available. This type of exercise normally does not reveal “holes” in a plan but will show where discrepancies exist in the preparation for the plan.

To examine the completeness of a plan, a different type of exercise needs to be conducted.
The simplest is a tabletop exercise in which participants sit around a table with a facilitator who supplies information related to the “incident” and the processes that are being examined.
Another type of exercise is a functional test in which certain aspects of a plan are tested to see how well they work (and how well prepared personnel are).

At the most extreme are full operational exercises designed to actually interrupt services in order to verify that all aspects of a plan are in place and sufficient to respond to the type of incident that is being simulated.

Slide 10



Principles of Computer Security, Fifth Edition

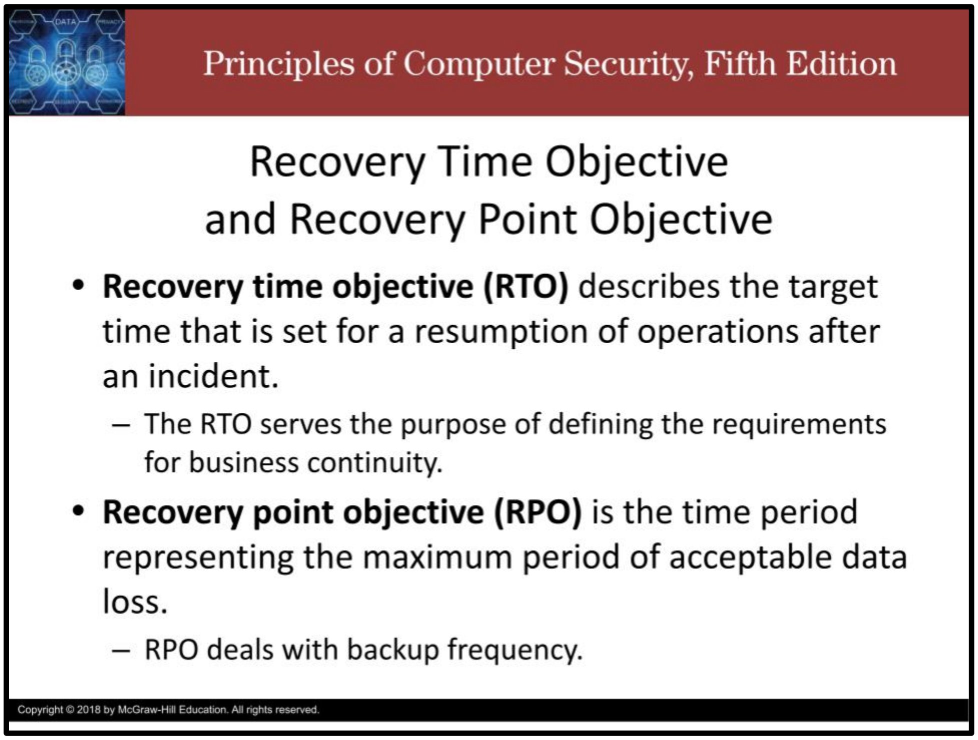
Test, Exercise, and Rehearse

- Tabletop exercises are a common form of exercising operational plans for senior management.
  - The senior management team, or elements of it, are gathered together and presented a scenario.
  - They can walk through their decision-making steps, communicate with others, and go through the motions of the exercise in the pattern in which they would likely be involved.
  - The scenario is presented at a level to test the responsiveness of their decisions and decision-making process.

Exercising operational plans is an effort that can take on many different forms.
For senior decision makers, the point of action is more typically a desk or a conference room, with their method being meetings and decisions.

A common form of exercising operational plans for senior management is the tabletop exercise.
The senior management team, or elements of it, are gathered together and presented a scenario.
They can walk through their decision-making steps, communicate with others, and go through the motions of the exercise in the pattern in which they would likely be involved.
The scenario is presented at a level to test the responsiveness of their decisions and decision-making process.

Slide 11



Principles of Computer Security, Fifth Edition

Recovery Time Objective and Recovery Point Objective

- **Recovery time objective (RTO)** describes the target time that is set for a resumption of operations after an incident.
  - The RTO serves the purpose of defining the requirements for business continuity.
- **Recovery point objective (RPO)** is the time period representing the maximum period of acceptable data loss.
  - RPO deals with backup frequency.

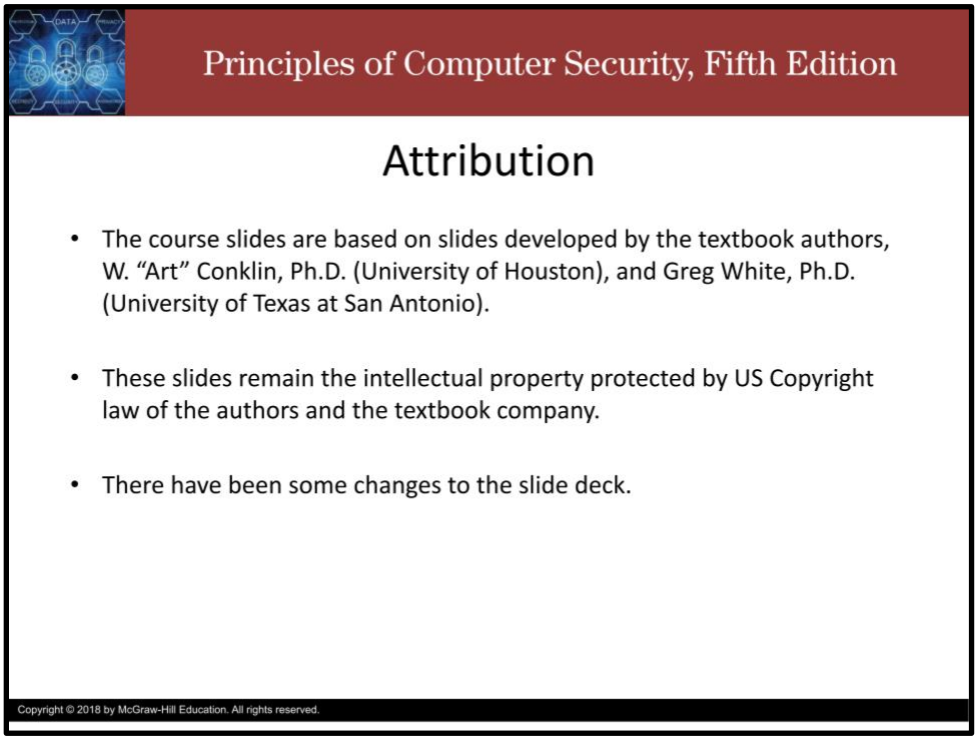
The term **recovery time objective (RTO)** is used to describe the target time that is set for a resumption of operations after an incident.
This is a period of time that is defined by the business, based on the needs of the enterprise.
A shorter RTO results in higher costs because it requires greater coordination and resources.

Recovery point objective (RPO), a totally different concept from RTO, is the time period representing the maximum period of acceptable data loss.
The RPO determines the frequency of backup operations necessary to prevent unacceptable levels of data loss.

RTO and RPO are seemingly related but in actuality measure different things entirely.
The RTO serves the purpose of defining the requirements for business continuity, while the RPO deals with backup frequency.

It is possible to have an RTO of 1 day and an RPO of 1 hour (can be inoperative for up to a day but can’t be without data for more than an hour), or an RTO of 1 hour and an RPO of 1 day (can’t be inoperative for more than 1 hour but can go without data for up to a day).
The determining factors are the needs of the business.

Slide 12



Principles of Computer Security, Fifth Edition

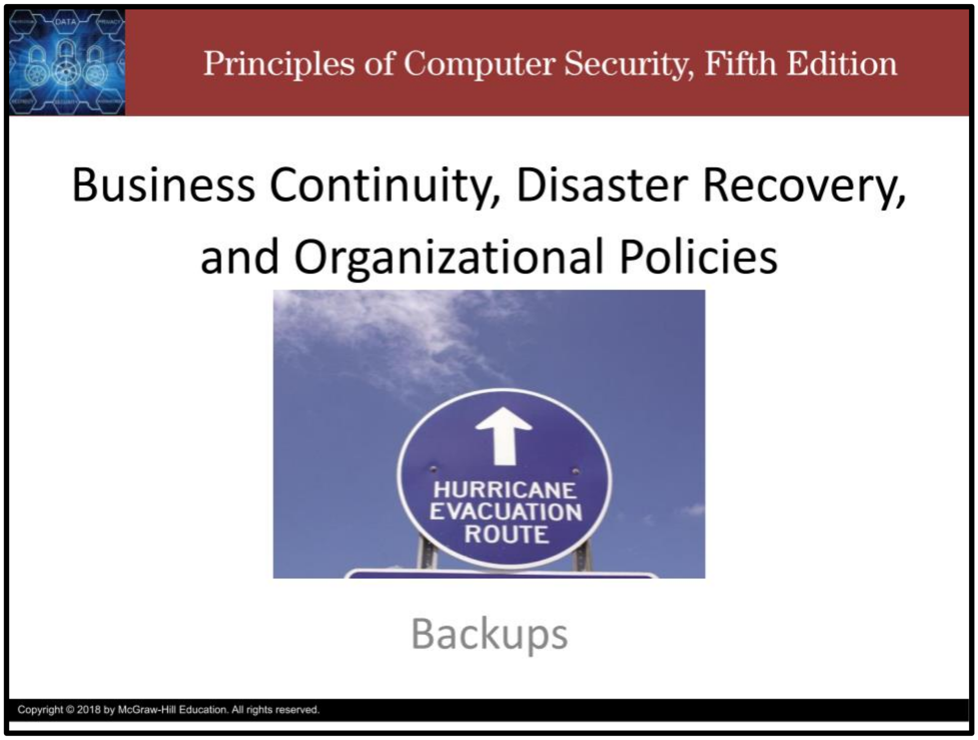
Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Thank you and take care.

Business Continuity, Disaster Recovery, and Organizational Policies: Backups

Slide 1



Principles of Computer Security, Fifth Edition

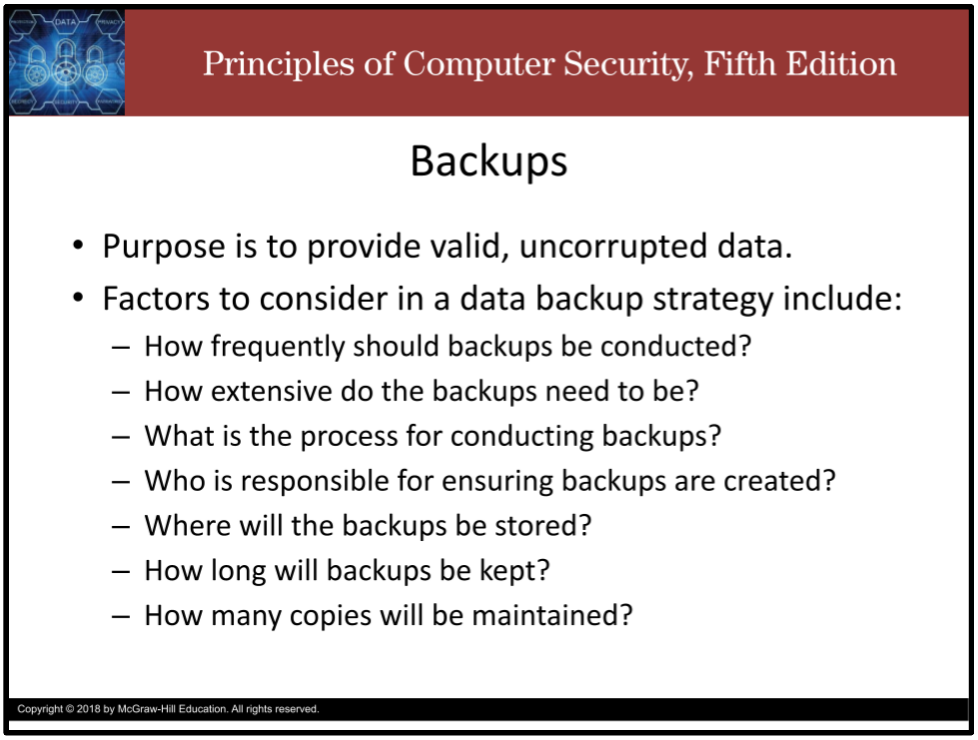
Business Continuity, Disaster Recovery, and Organizational Policies

HURRICANE
EVACUATION
ROUTE

Backups

Howdy! In this video, we discuss backups.

Slide 2



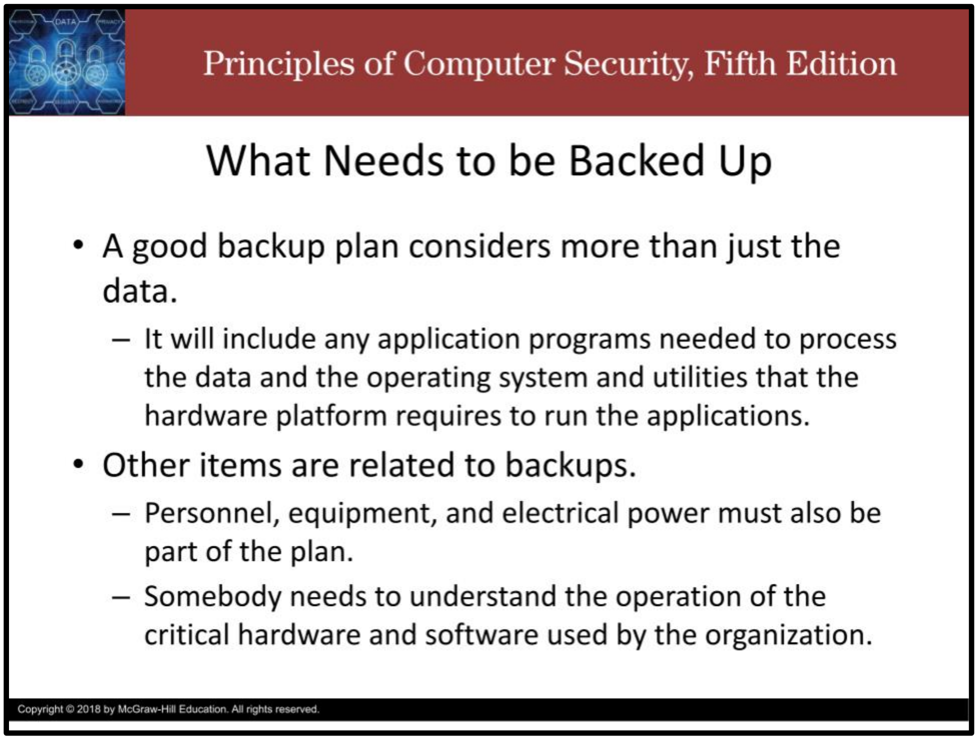
Principles of Computer Security, Fifth Edition

Backups

- Purpose is to provide valid, uncorrupted data.
- Factors to consider in a data backup strategy include:
  - How frequently should backups be conducted?
  - How extensive do the backups need to be?
  - What is the process for conducting backups?
  - Who is responsible for ensuring backups are created?
  - Where will the backups be stored?
  - How long will backups be kept?
  - How many copies will be maintained?

A key element in any business continuity or disaster recovery plan is the availability of backups. This is true not only because of the possibility of a disaster, but also because hardware and storage media will periodically fail, resulting in loss or corruption of critical data. An organization might also find backups critical when security measures have failed, and an individual has gained access to important information that may have become corrupted or at the very least can't be trusted. Data backup is thus a critical element in these plans, as well as in normal operation. The purpose of a backup is to provide valid, uncorrupted data in the event of corruption or loss of the original file or the media where the data was stored. Depending on the type of organization, legal requirements for maintaining backups can also affect how it is accomplished.

Slide 3



Principles of Computer Security, Fifth Edition

What Needs to be Backed Up

- A good backup plan considers more than just the data.
  - It will include any application programs needed to process the data and the operating system and utilities that the hardware platform requires to run the applications.
- Other items are related to backups.
  - Personnel, equipment, and electrical power must also be part of the plan.
  - Somebody needs to understand the operation of the critical hardware and software used by the organization.

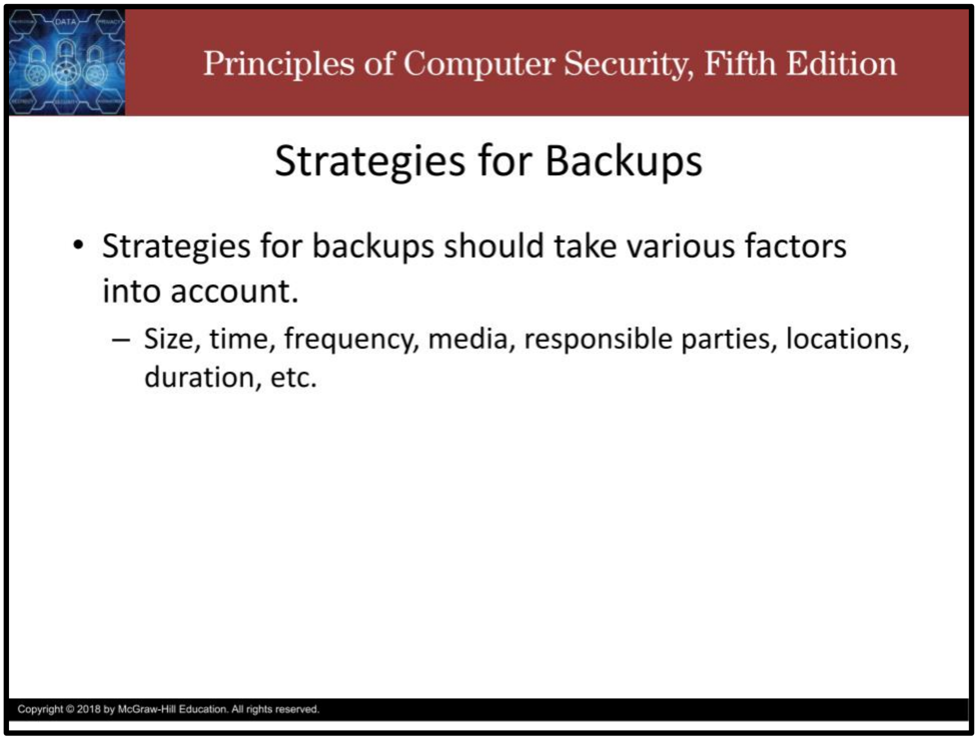
Backups are typically made of the data that an organization relies on to conduct its daily operations. While this is certainly essential, a good backup plan will consider more than just the data; it will also include any software needed to process the data and the operating system and utilities that the hardware platform requires to run the applications.

The business continuity or disaster recovery plan should also address other items related to backups, such as personnel, equipment, and electrical power.

Somebody needs to understand the operation of the critical hardware and software used by the organization.

If the disaster that destroyed the original copy of the data and the original systems also results in the loss of the only personnel who know how to process the data, having backup data will not be enough to restore normal operations for the organization. Similarly, if the data requires specific software to be run on a very specific hardware platform, then having the data without the application program or required hardware will also not be sufficient.

Slide 4



Principles of Computer Security, Fifth Edition

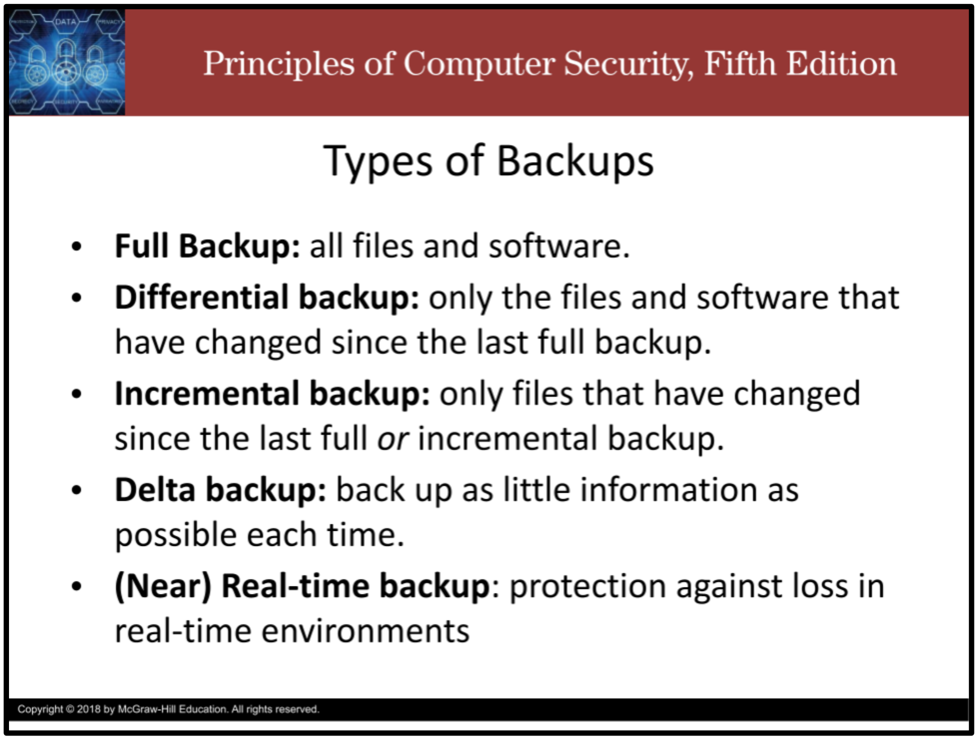
Strategies for Backups

- Strategies for backups should take various factors into account.
  - Size, time, frequency, media, responsible parties, locations, duration, etc.

The process for creating a backup copy of data and software requires more thought than simply stating “copy all required files.” The size of the resulting backup must be considered, as well as the time required to conduct the backup. Both of these will affect details such as how frequently the backup will occur and the type of storage medium that will be used for the backup.

Other considerations include who will be responsible for conducting the backup, where the backups will be stored, and how long they should be maintained. Short-term storage for accidentally deleted files that users need to have restored should probably be close at hand. Longer-term storage for backups that may be several months or even years old should occur in a different facility. It should be evident by now that even something that sounds as simple as maintaining backup copies of essential data requires careful consideration and planning.

Slide 5



Principles of Computer Security, Fifth Edition

Types of Backups

- **Full Backup:** all files and software.
- **Differential backup:** only the files and software that have changed since the last full backup.
- **Incremental backup:** only files that have changed since the last full *or* incremental backup.
- **Delta backup:** back up as little information as possible each time.
- **(Near) Real-time backup**: protection against loss in real-time environments

There are four basic types of backups.

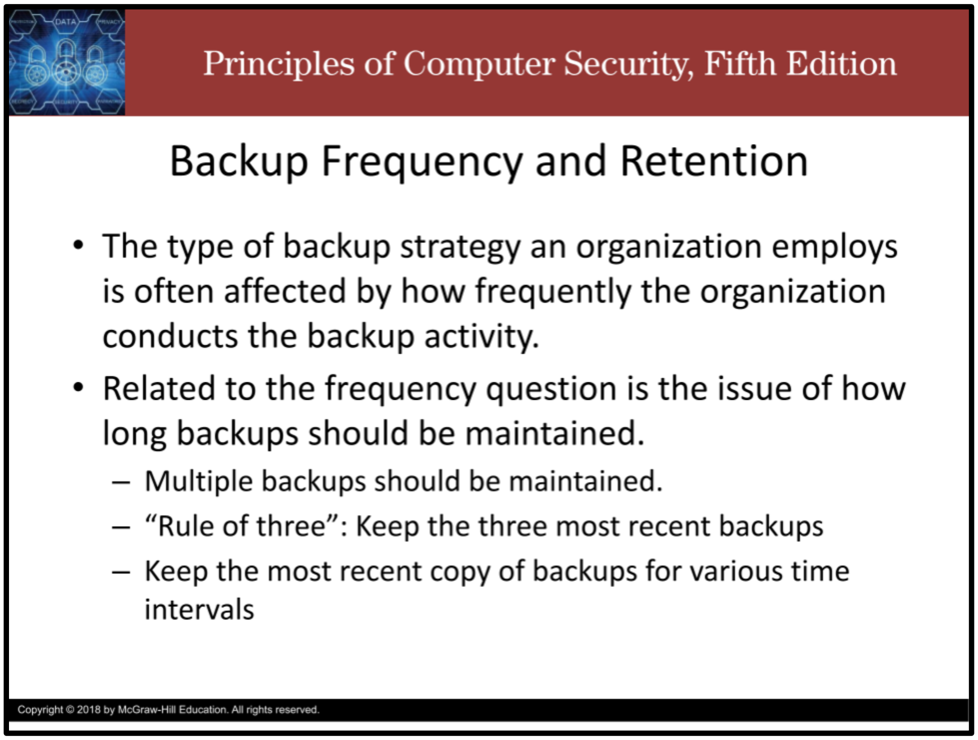
In **a full backup**, all files and software are copied onto the storage media.
In a **differential backup**, only the files and software that have changed since the last full backup was completed are backed up.

The **incremental backup** backs up only files that have changed since the last full *or* incremental backup occurred, thus requiring fewer files to be backed up.

The goal of the **delta backup** is to back up as little information as possible each time you perform a backup.

There are newer backup methods similar to delta backups that minimize what is backed up. Real-time or near-real-time backup strategies (such as journaling, transactional backups, and electronic vaulting) provide protection against loss in real-time environments. Implementing these methods into an overall backup strategy can increase options and flexibility during times of recovery.

Slide 6



Principles of Computer Security, Fifth Edition

Backup Frequency and Retention

- The type of backup strategy an organization employs is often affected by how frequently the organization conducts the backup activity.
- Related to the frequency question is the issue of how long backups should be maintained.
  - Multiple backups should be maintained.
  - “Rule of three”: Keep the three most recent backups
  - Keep the most recent copy of backups for various time intervals

The type of backup strategy an organization employs is often affected by how frequently the organization conducts the backup activity.
The longer it has been since the backup was created, the more changes that likely will have occurred, and the more useful the backup. There is no easy answer, however, to how frequently an organization should perform backups. Every organization should consider how long it can survive without current data from which to operate. It can then determine how long it will take to restore from backups, using various methods, and decide how frequently backups need to occur. This sounds simple, but it is a serious, complex decision to make.

Related to the frequency question is the issue of how long backups should be maintained. Is it sufficient to simply maintain a single backup from which to restore data? Security professionals will tell you no; multiple backups should be maintained, for a variety of reasons. If the reason for restoring from the backup is the discovery of an intruder in the system, it is important to restore the system to its pre-intrusion state.

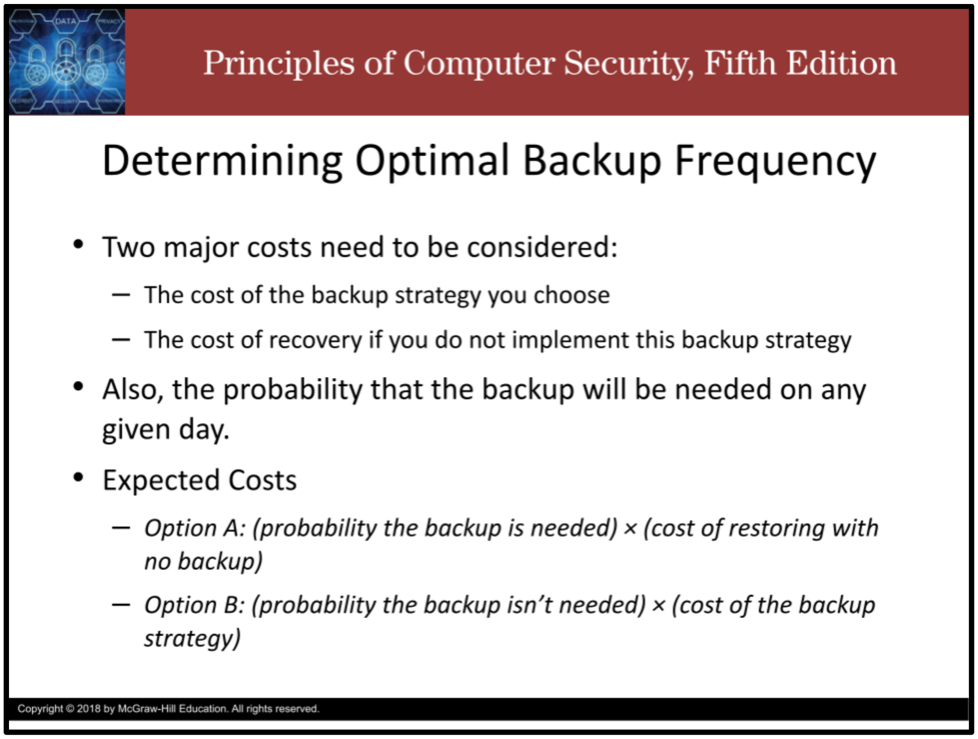
If the intruder has been in the system for several months before being discovered, and backups are taken weekly, it will not be possible to restore to a pre-intrusion state if only one backup is maintained.

This would mean that all data and system files would be suspect and may not be reliable.

If multiple backups were maintained, at various intervals, then it is easier to return to a point before the intrusion (or before the security or operational event that is necessitating the restoration) occurred.

There are several strategies or approaches to backup retention. One common and easy-to-remember strategy is the “rule of three,” in which the three most recent backups are kept. When a new backup is created, the oldest backup is overwritten. Another strategy is to keep the most recent copy of backups for various time intervals. For example, you might keep the latest daily, weekly, monthly, quarterly, and yearly backups. Note that in certain environments, regulatory issues may prescribe a specific frequency and retention period, so it is important to know your organization's requirements when determining how often you will create a backup and how long you will keep it.

Slide 7



Principles of Computer Security, Fifth Edition

Determining Optimal Backup Frequency

- Two major costs need to be considered:
  - The cost of the backup strategy you choose
  - The cost of recovery if you do not implement this backup strategy
- Also, the probability that the backup will be needed on any given day.
- Expected Costs
  - *Option A: (probability the backup is needed) × (cost of restoring with no backup)*
  - *Option B: (probability the backup isn't needed) × (cost of the backup strategy)*

In determining the optimal backup frequency, two major costs need to be considered: the cost of the backup strategy you choose and the cost of recovery if you do not implement this backup strategy (that is, if no backups were created). You must also factor into this equation the probability that the backup will be needed on any given day. Thus, there are two expected costs to consider:

Option A: (probability the backup is needed) × (cost of restoring with no backup)
and
Option B: (probability the backup isn't needed) × (cost of the backup strategy)

Option A is the loss you can expect if your organization has no backup. Option B is the amount you expect to spend to ensure that you can restore, should a problem occur (think of this as backup insurance—the cost of an insurance policy that may never be used but that you are willing to pay for, just in case).

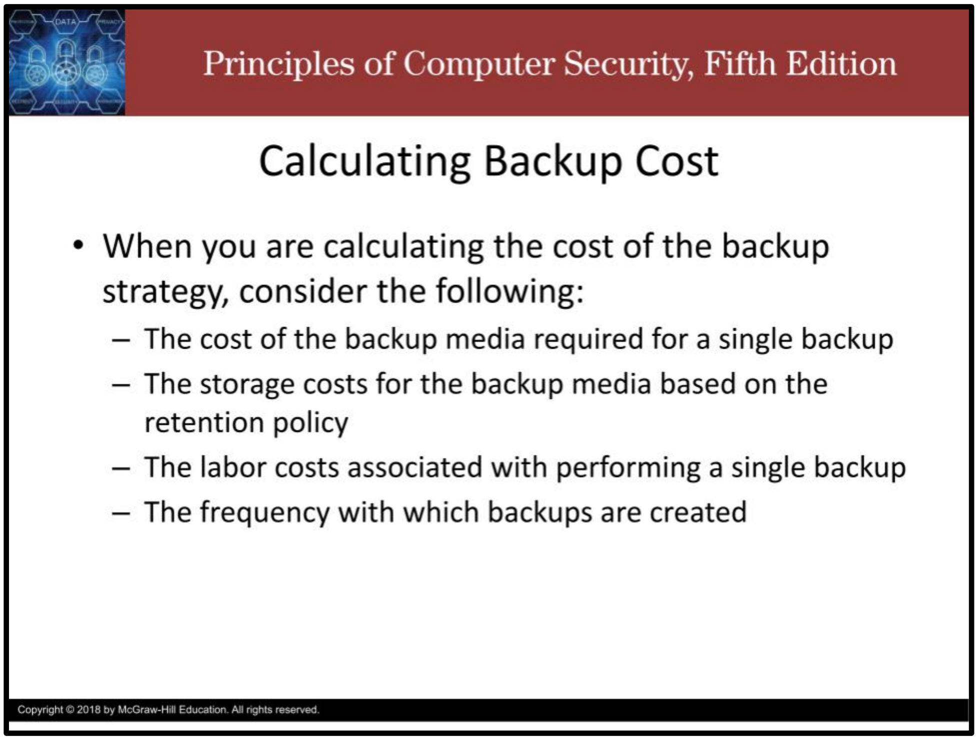
The optimal backup frequency is the one which minimizes the cost of Option B, where the frequency impacts both the probability that the backup is needed and the cost of the strategy. The more often the data is backed up, the more expensive it is, but more importantly, the less data there will be that was not included in the most recent backup.

For example, if the probability of a backup being needed is 10 percent, and the cost of restoring with no backup is $100,000, then Option A would yield a figure of $10,000. This can be compared with the alternative Option B, which would be a 90 percent chance the backup is not needed multiplied by the cost of implementing your backup strategy (of taking and maintaining the backups), which is, say, $10,000 annually. Option B comes out to $9000. In this example, the cost of maintaining the backup is less than the cost of not having backups, so Option B would be the rational choice. While this is an easy trade-off to understand, in reality it is often difficult to accurately determine the probability of a backup being needed.

Fortunately, the figures for the potential loss if there is no backup are generally so much greater than the cost of maintaining a backup that a mistake in judging the probability will not matter—it just makes too much sense to maintain backups. This example also uses a straight comparison based solely on the cost of the process of restoring with and without a backup strategy. What needs to be included in the cost of both of these is the loss that occurs while the asset is not available as it is being restored—in essence, a measurement of the value of the asset itself.

When working with these two calculations, you have to remember that this is a cost-avoidance exercise. The organization is not going to increase revenues with its backup strategy. The goal is to minimize the potential loss due to some catastrophic event by creating a backup strategy that will address your organization’s needs. This is, probably, one of the most frustrating parts of a security professional’s job: convincing upper management to spend money on security, where the main benefit to the bottom line is that _should_ something bad happen, the loss will be less than if less or no security protections had been applied.

Slide 8



Principles of Computer Security, Fifth Edition

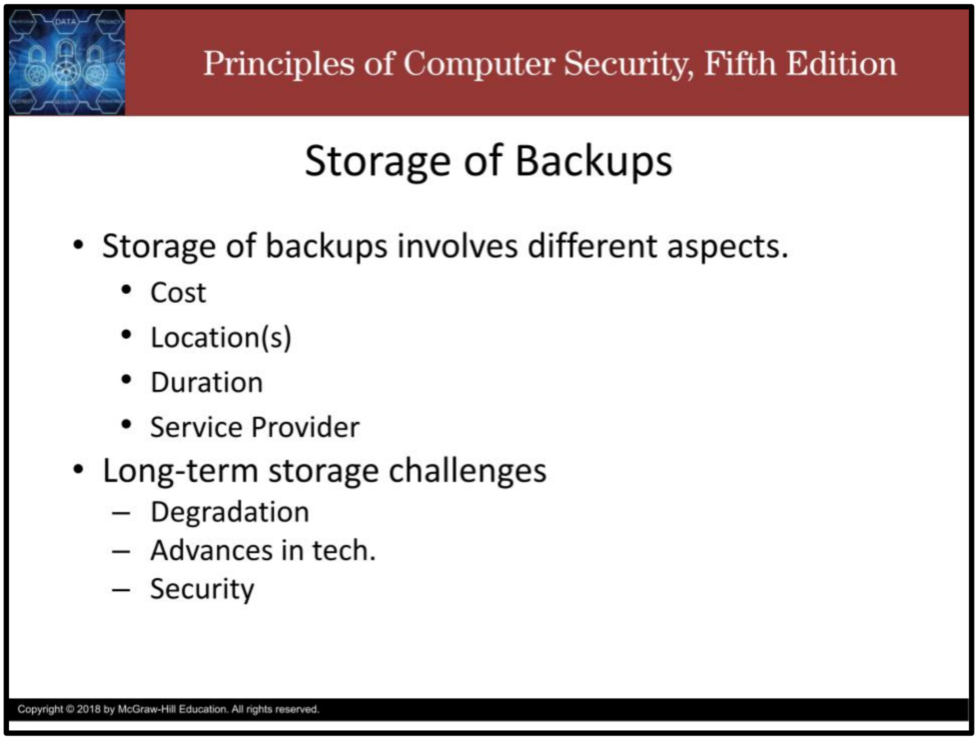
Calculating Backup Cost

- When you are calculating the cost of the backup strategy, consider the following:
  - The cost of the backup media required for a single backup
  - The storage costs for the backup media based on the retention policy
  - The labor costs associated with performing a single backup
  - The frequency with which backups are created

When you are calculating the cost of the backup strategy, you must consider:

The cost of the backup media required for a single backup, the storage costs for the backup media based on the retention policy, the labor costs associated with performing a single backup, and the frequency with which backups are created. All of these considerations can be used to arrive at an annual cost for implementing your chosen backup strategy, and this is the number that goes into the computation for Option B (B for backup).

Slide 9



Principles of Computer Security, Fifth Edition

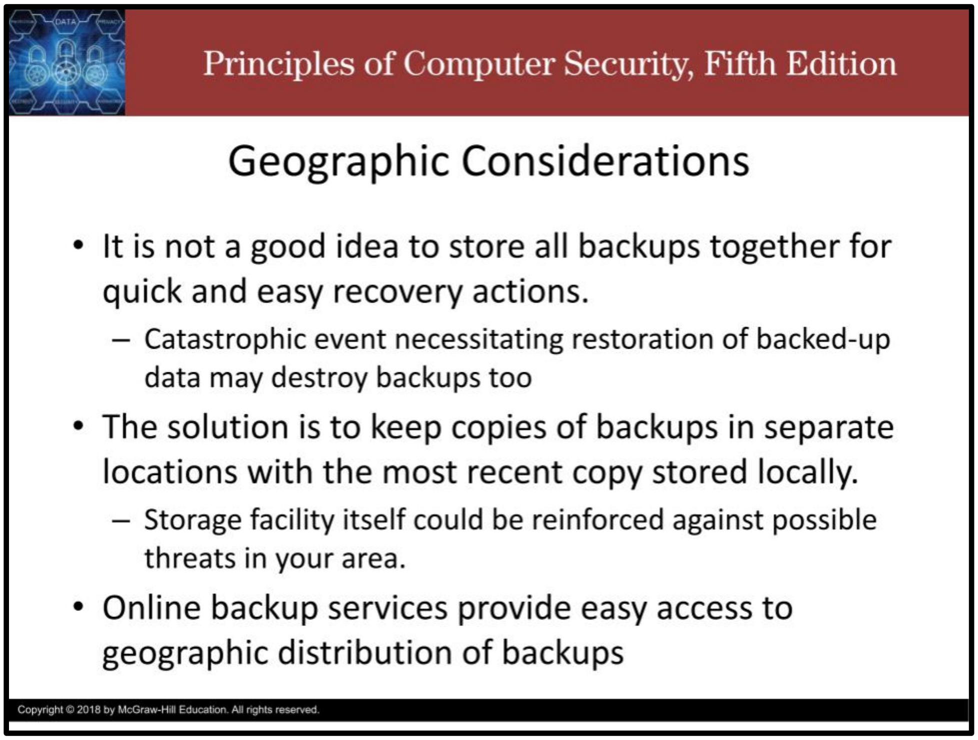
Storage of Backups

- Storage of backups involves different aspects.
  - Cost
  - Location(s)
  - Duration
  - Service Provider
- Long-term storage challenges
  - Degradation
  - Advances in tech.
  - Security

There are several different aspects involved in the storage of backups, such as the cost, location, duration, and service provider.

Long-term storage of backups presents particular challenges. Degradation of the media is a distinct possibility and needs to be considered. Another consideration is advances in technology as the media you used to store your data two years ago may now be considered obsolete. Software applications evolve, and the media may be present but may not be compatible with current versions of the software. A security related challenge is that more than one employee in the company should know the key to decrypt the files. If only one person knows it, then you are dangerously close to no one knowing it and those backups being useless.

Slide 10



Principles of Computer Security, Fifth Edition

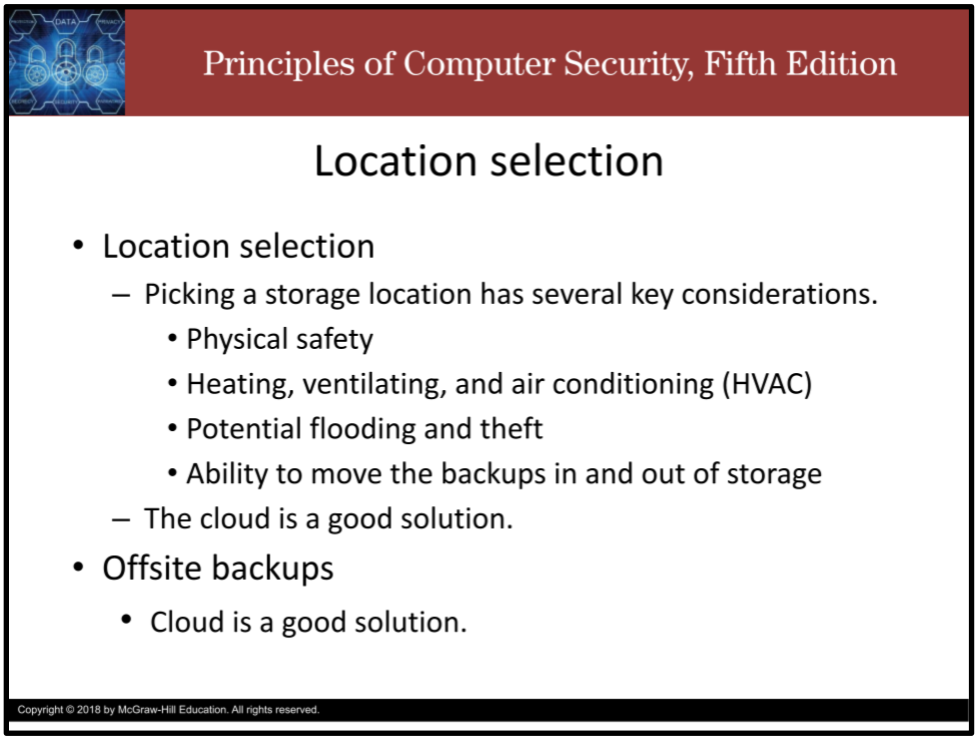
Geographic Considerations

- It is not a good idea to store all backups together for quick and easy recovery actions.
  - Catastrophic event necessitating restoration of backed-up data may destroy backups too
- The solution is to keep copies of backups in separate locations with the most recent copy stored locally.
  - Storage facility itself could be reinforced against possible threats in your area.
- Online backup services provide easy access to geographic distribution of backups

Where should you store the backups? On-site, right? That way it’s quick and easy to do the backups and if you need to restore, the backups are right there, ready to go. Not so fast. It is not a good idea to store all backups together for quick and easy recovery actions. A catastrophic event that necessitated restoring data from backups may also destroy the backups too.

The solution is to keep copies of backups in geographically separate locations with only the most recent copy stored locally. The storage facility which holds the backups should be reinforced against threats in the area (both terrestrial and celestial… I’m talking weather, bad guys, and meteors). Cloud backup services are an easy way to get geographic distribution of backups without the overhead of managing a global portfolio of data storage houses.

Slide 11



Principles of Computer Security, Fifth Edition

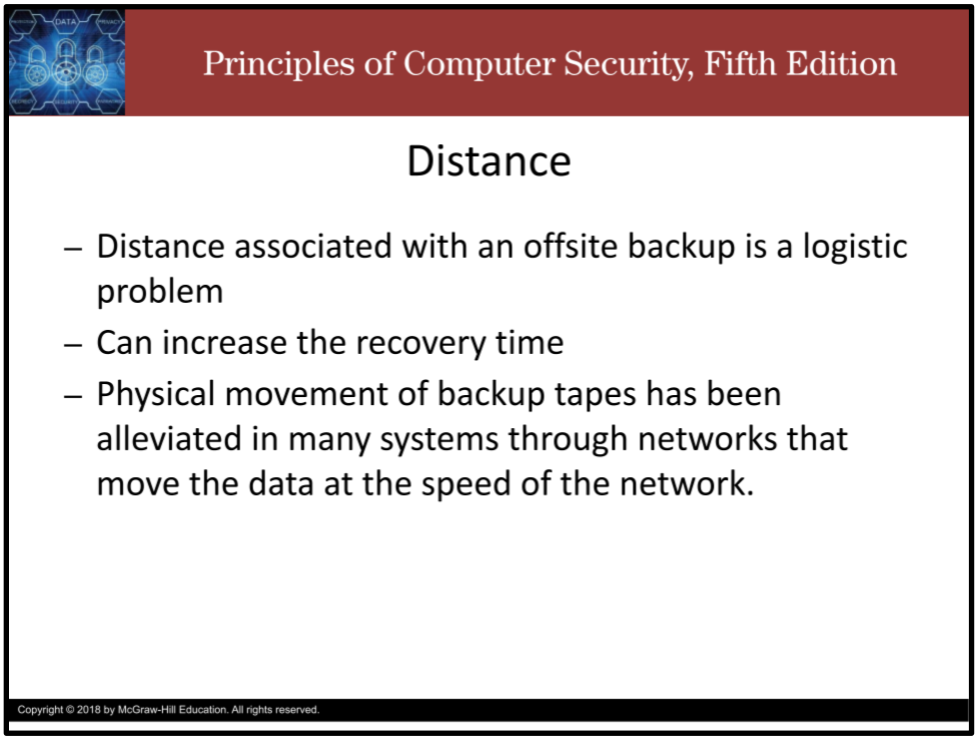
Location selection

- Location selection
  - – Picking a storage location has several key considerations.
    - Physical safety
    - Heating, ventilating, and air conditioning (HVAC)
    - Potential flooding and theft
    - Ability to move the backups in and out of storage
  - – The cloud is a good solution.
- Offsite backups
  - Cloud is a good solution.

Picking a storage location has several key considerations, such as physical safety, heating, ventilating, and air conditioning (HVAC), potential flooding and theft, and the ability to move the backups in and out of storage.

Used properly, the cloud is a good solution since networks are fast, storage is cheap and reliable, and encryption is available. Offsite backups are backups stored offsite. This is important to mitigate the risk of backups stored at the main site being destroyed at the same time as onsite backups are destroyed due to some catastrophe. Again. The cloud is a good option.

Slide 12



Principles of Computer Security, Fifth Edition

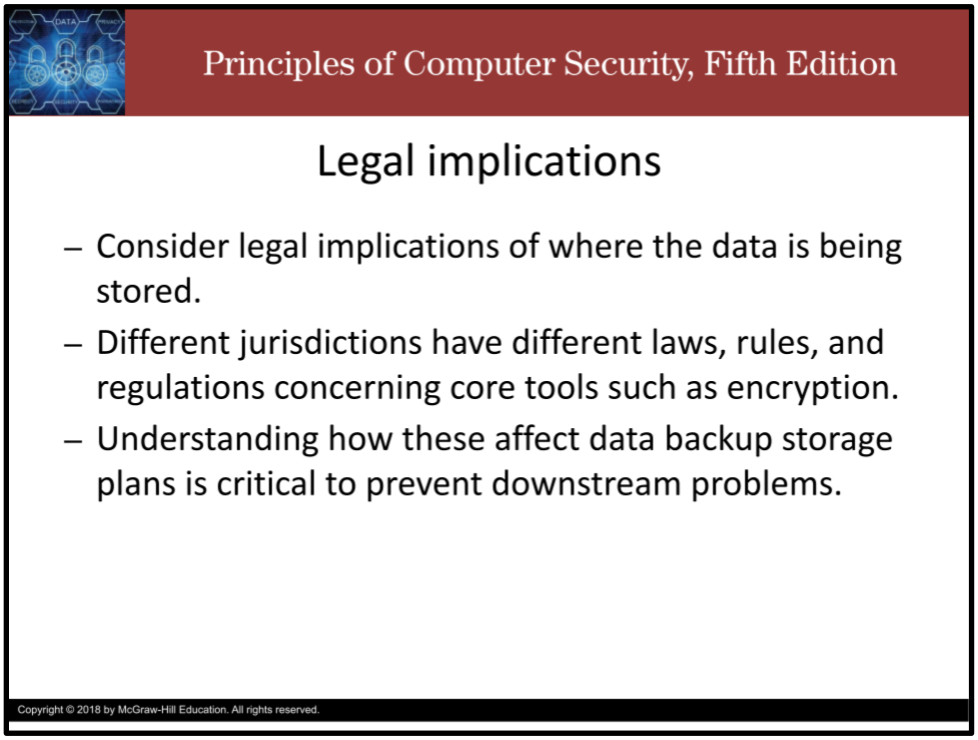
Distance

- Distance associated with an offsite backup is a logistic problem
- Can increase the recovery time
- Physical movement of backup tapes has been alleviated in many systems through networks that move the data at the speed of the network.

The distance associated with an offsite backup is a logistic problem. If the backups are on physical media and stored at a site several hours away, this will add to the recovery time.

The bottleneck of physical movement of backup media has been alleviated in many systems through networks that move the data at the speed of the network.

Slide 13



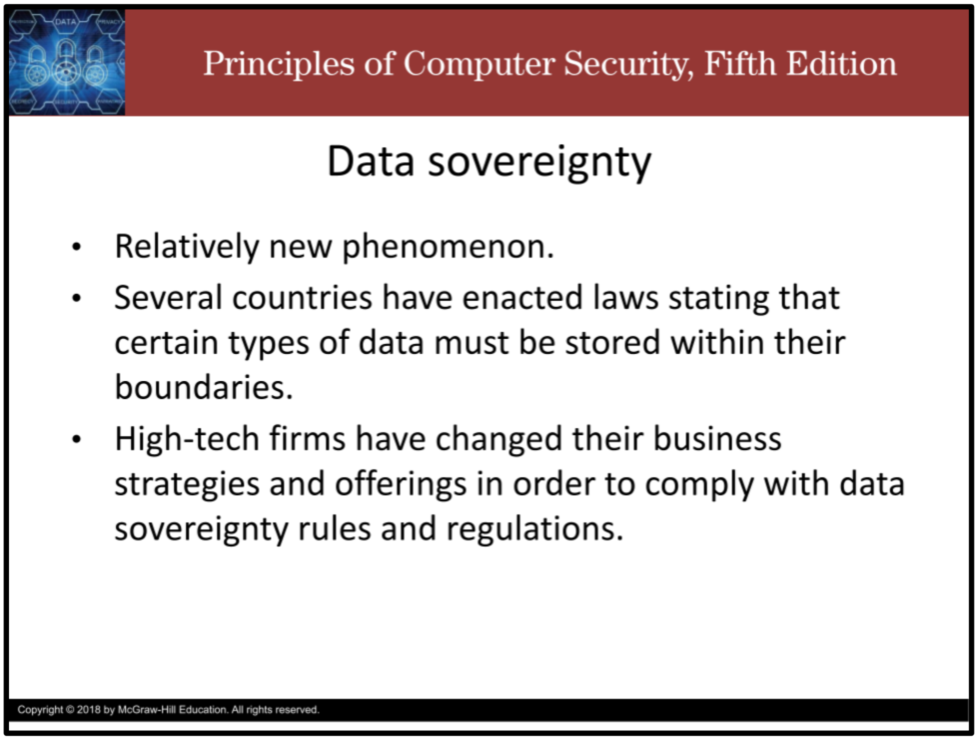
Principles of Computer Security, Fifth Edition

Legal implications

- Consider legal implications of where the data is being stored.
- Different jurisdictions have different laws, rules, and regulations concerning core tools such as encryption.
- Understanding how these affect data backup storage plans is critical to prevent downstream problems.

You must consider the legal implications of where data is being stored.
Different places have different rules and regulations.
Understanding how these rules and regulations affect data backup storage plans is critical to prevent downstream problems.

Slide 14



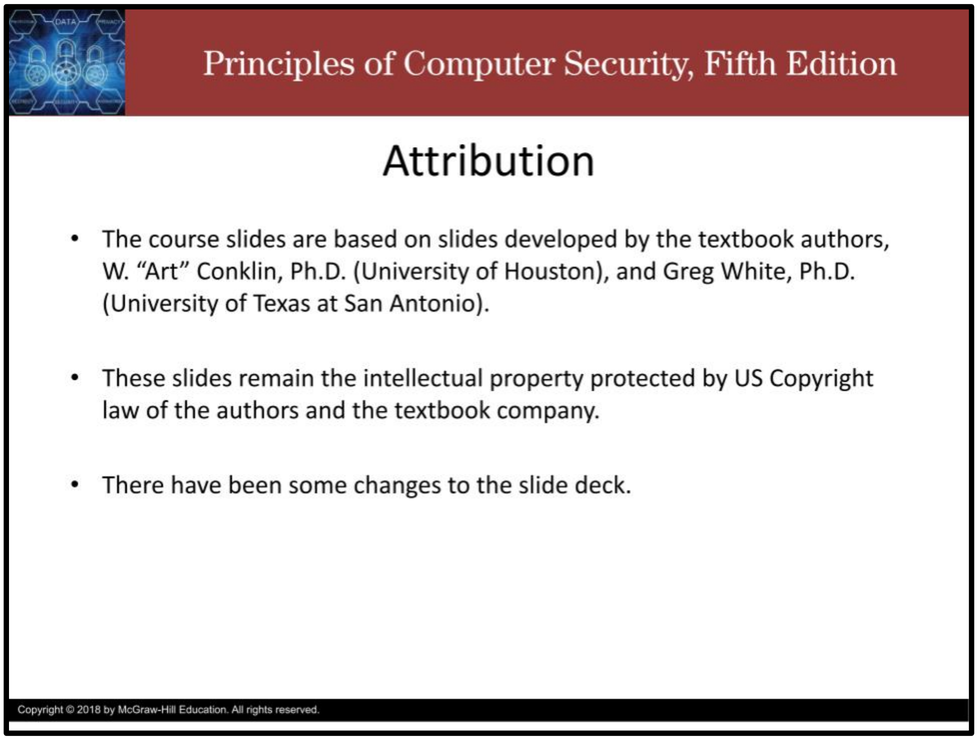
Principles of Computer Security, Fifth Edition

Data sovereignty

- Relatively new phenomenon.
- Several countries have enacted laws stating that certain types of data must be stored within their boundaries.
- High-tech firms have changed their business strategies and offerings in order to comply with data sovereignty rules and regulations.

Data sovereignty is a relatively new phenomenon, but in the past couple of years several countries have enacted laws stating that certain types of data must be stored within their boundaries.
This is a problem with an Internet without borders.
Several high-tech firms have changed their business strategies and offerings in order to comply with data sovereignty rules and regulations.
For example, LinkedIn abandoned the Russian market after Russia told it to store data on Russian citizens on Russian servers, something which LinkedIn was unwilling to do.

Slide 15



Principles of Computer Security, Fifth Edition

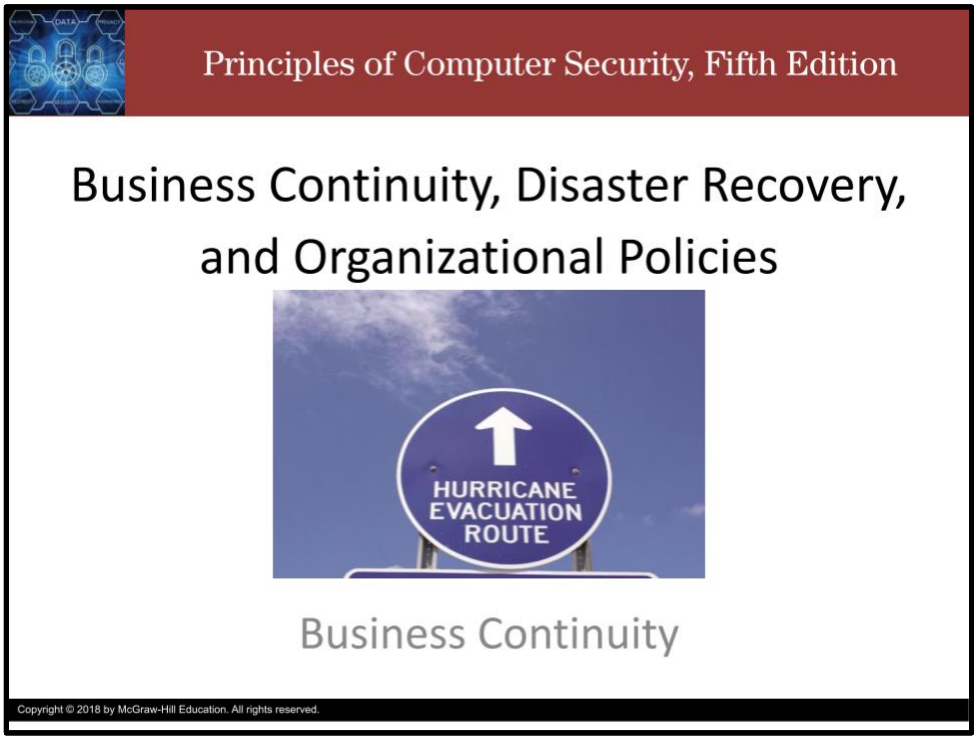
Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Thank you and take care.

Business Continuity, Disaster Recovery, and Organizational Policies: Business Continuity

Slide 1



Principles of Computer Security, Fifth Edition

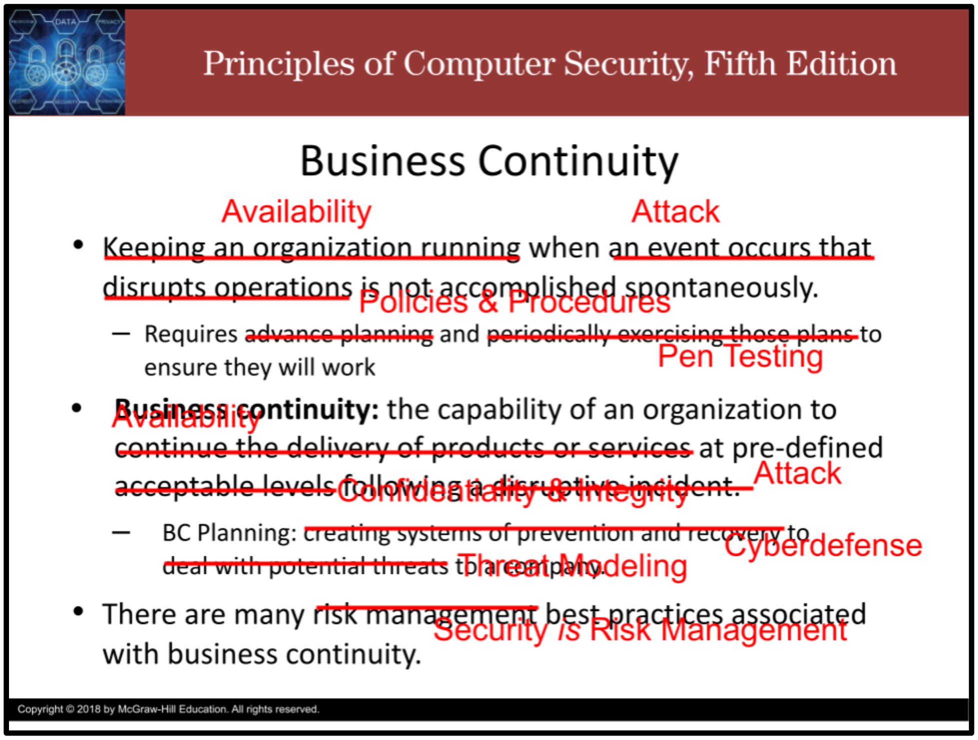
Business Continuity, Disaster Recovery, and Organizational Policies

HURRICANE
EVACUATION
ROUTE

Business Continuity

Howdy! In this video, we discuss business continuity.

Slide 2



Principles of Computer Security, Fifth Edition

Business Continuity

Availability Attack

- Keeping an organization running when an event occurs that disrupts operations is not accomplished spontaneously.
  Policies & Procedures
  - Requires ~~advance planning~~ and ~~periodically exercising those plans~~ to ensure they will work
    Pen Testing
- **Business continuity:** the capability of an organization to ~~continue the delivery of products or services~~ at pre-defined ~~acceptable levels following a disruptive incident.~~
  Availability Confidentiality & Integrity Attack
  - BC Planning: ~~creating systems of prevention and recovery~~ to ~~deal with potential threats~~ to a company.
    Cyberdefense Threat Modeling
- There are many ~~risk management~~ best practices associated with business continuity.
  Security *is* Risk Management

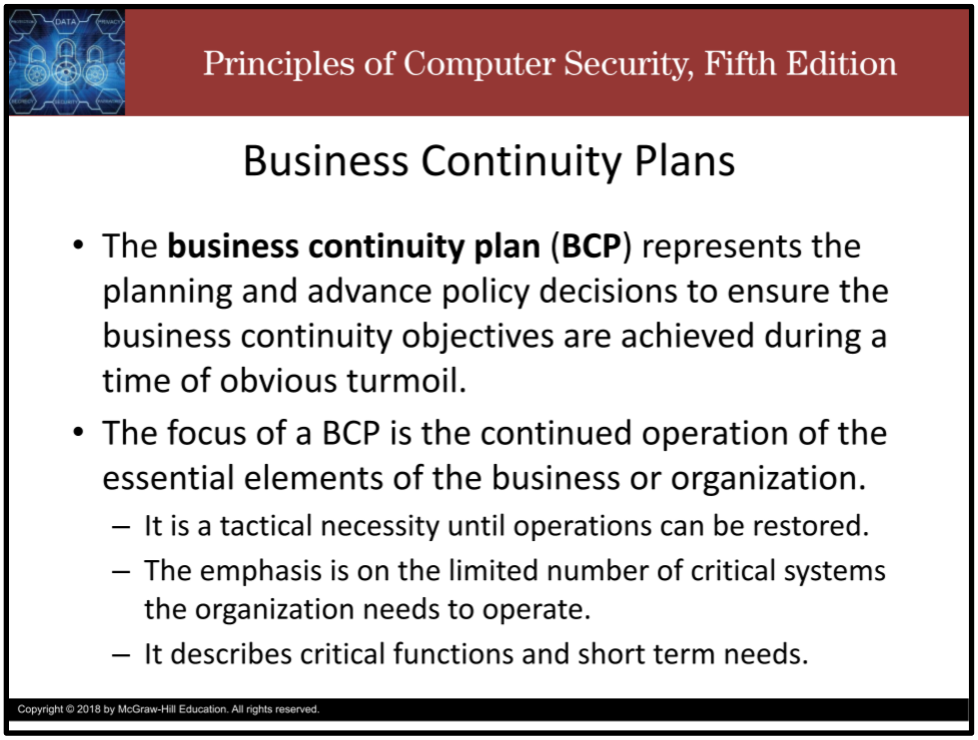
Keeping an organization running when a disruptive event occurs is not a spontaneous accomplishment. It requires planning in advance and periodically testing, exercising, and rehearsing those plans to ensure they will work.

Business continuity is "the capability of an organization to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident."
Business continuity planning is the process of creating systems of prevention and recovery to deal with potential threats to a company.
There are many risk management best practices associated with business continuity planning.

Can you spot the security connections?

Yeah. If you like business and you want to continue doing it, you need to build security into the business. Cybersecurity focuses on the security of connected devices. Business continuity is more like security at large, the security of the whole organization, against threats that may have nothing to do with connected devices and against which cyberdefense mechanisms are ineffective. But, with so much business today relying on connected devices, it's a safe bet that a significant portion of the business continuity plan should be devoted to cybersecurity.

Slide 3



Principles of Computer Security, Fifth Edition

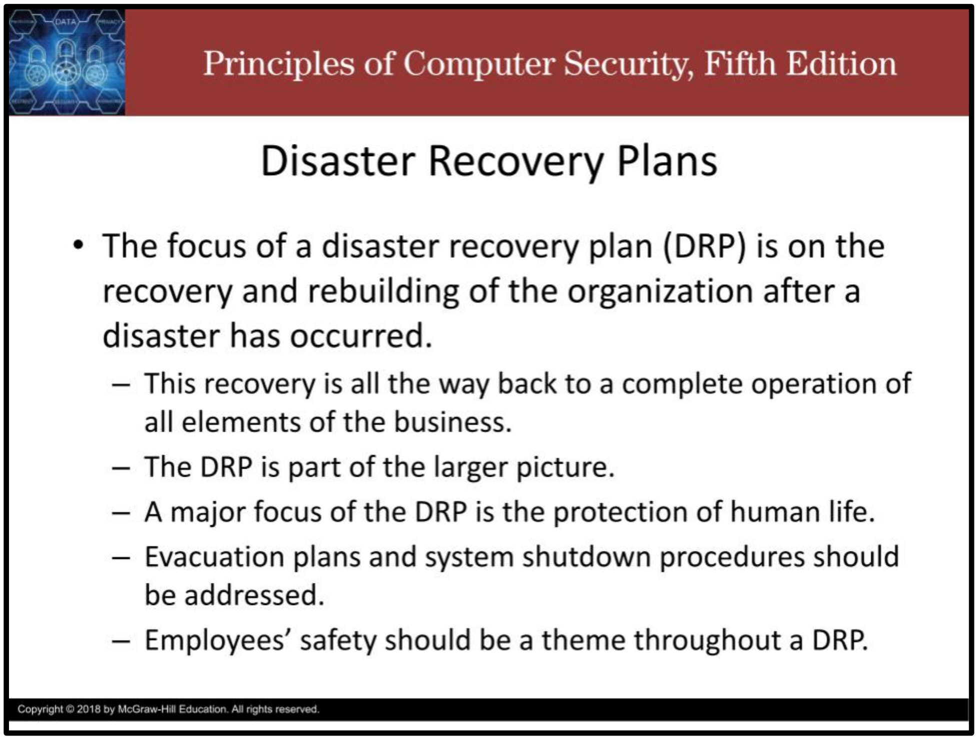
Business Continuity Plans

- The **business continuity plan** (**BCP**) represents the planning and advance policy decisions to ensure the business continuity objectives are achieved during a time of obvious turmoil.
- The focus of a BCP is the continued operation of the essential elements of the business or organization.
  - It is a tactical necessity until operations can be restored.
  - The emphasis is on the limited number of critical systems the organization needs to operate.
  - It describes critical functions and short term needs.

You might wonder what the difference is between a disaster recovery plan and a **business continuity plan**—after all, isn't the purpose of disaster recovery the continued operation of the organization or business during a period of disruption? Many times, these two terms are sometimes used synonymously, and for many organizations there may be no major difference in the two. There are, however, real differences between a BCP and a DRP, one of which is the *focus*.

The focus of a BCP is the continued operation of the essential elements of the business or organization. The BCP is a tactical necessity until operations can be restored. The emphasis is on the limited number of critical systems that the organization needs in order to operate. The BCP describes the critical functions, the order in which they should be returned to operation, and the short term operational needs.

Slide 4



Principles of Computer Security, Fifth Edition

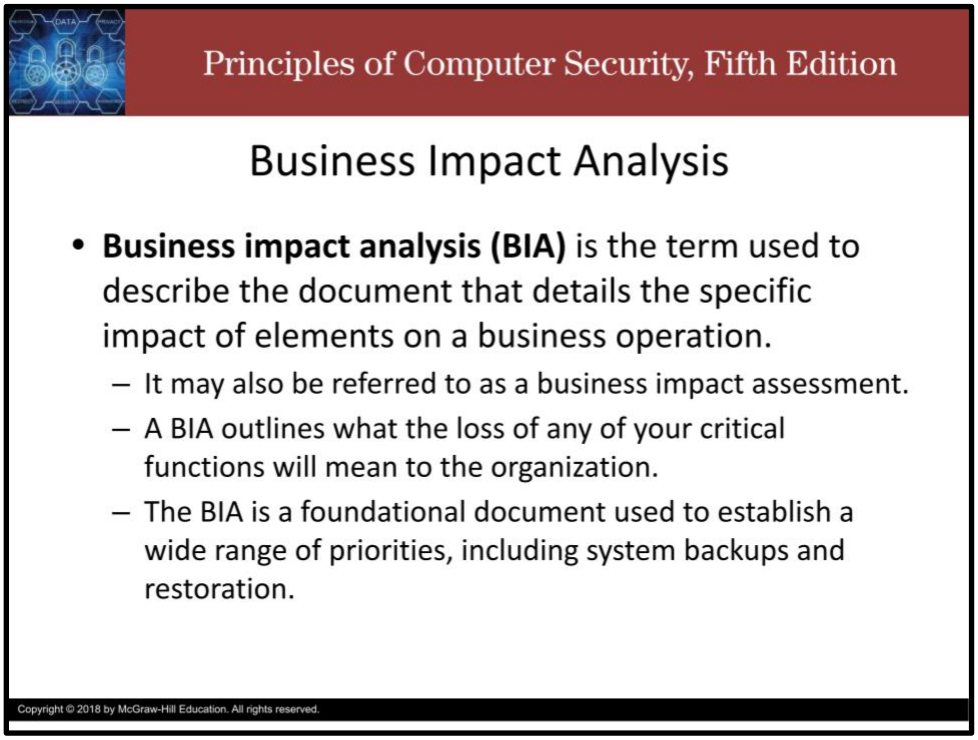
Disaster Recovery Plans

- The focus of a disaster recovery plan (DRP) is on the recovery and rebuilding of the organization after a disaster has occurred.
  - This recovery is all the way back to a complete operation of all elements of the business.
  - The DRP is part of the larger picture.
  - A major focus of the DRP is the protection of human life.
  - Evacuation plans and system shutdown procedures should be addressed.
  - Employees’ safety should be a theme throughout a DRP.

The focus of a disaster recovery plan (DRP) is on the recovery and rebuilding of the organization after a disaster has occurred. The goal of the recovery is to restore complete operation of all elements of the business. Whereas a BCP focuses on keeping the business alive, a DRP focuses on the larger picture of returning the business to thriving.

Speaking of staying alive, a major focus of the DRP is the protection of human life, meaning evacuation plans and system shutdown procedures should be addressed. Human resources are the most valuable assets of the business. If you can’t (or won’t) take care of your employees (especially during a disaster), you’re not a business, you’re a parasite. Employee safety should be a theme throughout a DRP.

Slide 5



Principles of Computer Security, Fifth Edition

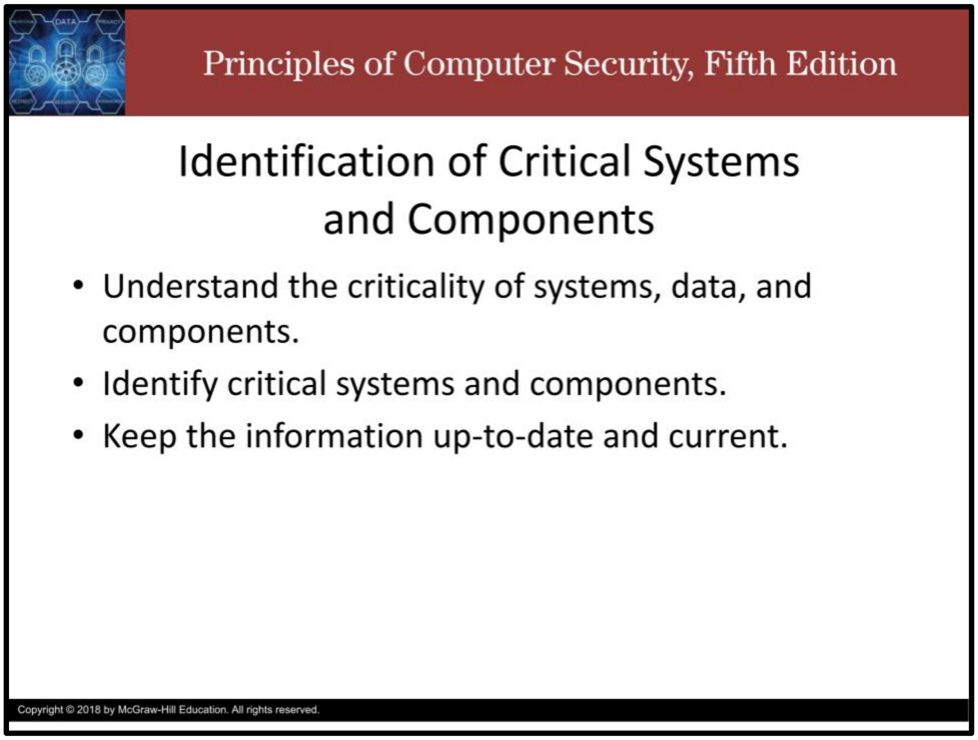
Business Impact Analysis

- **Business impact analysis (BIA)** is the term used to describe the document that details the specific impact of elements on a business operation.
  - It may also be referred to as a business impact assessment.
  - A BIA outlines what the loss of any of your critical functions will mean to the organization.
  - The BIA is a foundational document used to establish a wide range of priorities, including system backups and restoration.

A **Business impact analysis (BIA)** is a document that details the specific impact of elements on a business operation. It may also be referred to as a business impact assessment. A BIA outlines what the loss of any of your critical functions will mean to the organization.

It is a foundational document used to establish a wide range of priorities, including system backups and restoration, which are needed in maintaining continuity of operation, and more. While each person may consider their individual tasks to be important, the **BIA** is a business-level analysis of the criticality of all elements with respect to the business as a whole. The BIA will take into account the increased risk from minimal operations, and is designed to determine and justify what is essentially critical for a business to survive versus what someone may state or wish.

Slide 6



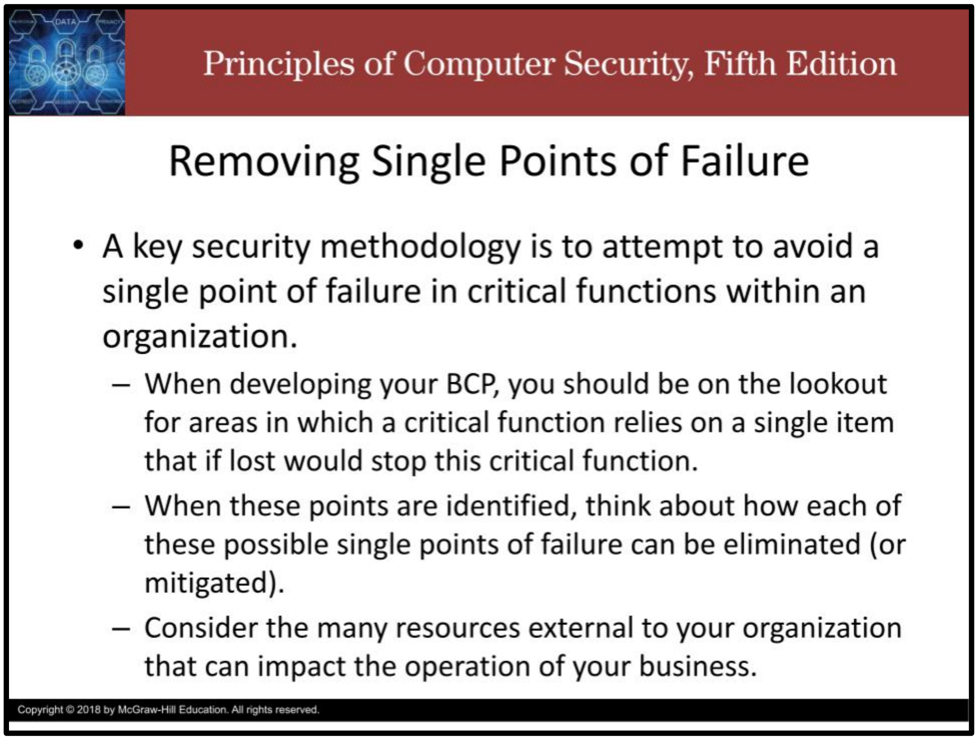
Principles of Computer Security, Fifth Edition

Identification of Critical Systems and Components

- Understand the criticality of systems, data, and components.
- Identify critical systems and components.
- Keep the information up-to-date and current.

A foundational element of a security plan is an understanding of the criticality of systems, the data, and the components. Identifying the critical systems and components is one of the first steps an organization needs to undertake in designing the set of security controls. As the systems evolve and change, the continued identification of the critical systems needs to occur, keeping the information up-to-date and current.

Slide 7



Principles of Computer Security, Fifth Edition

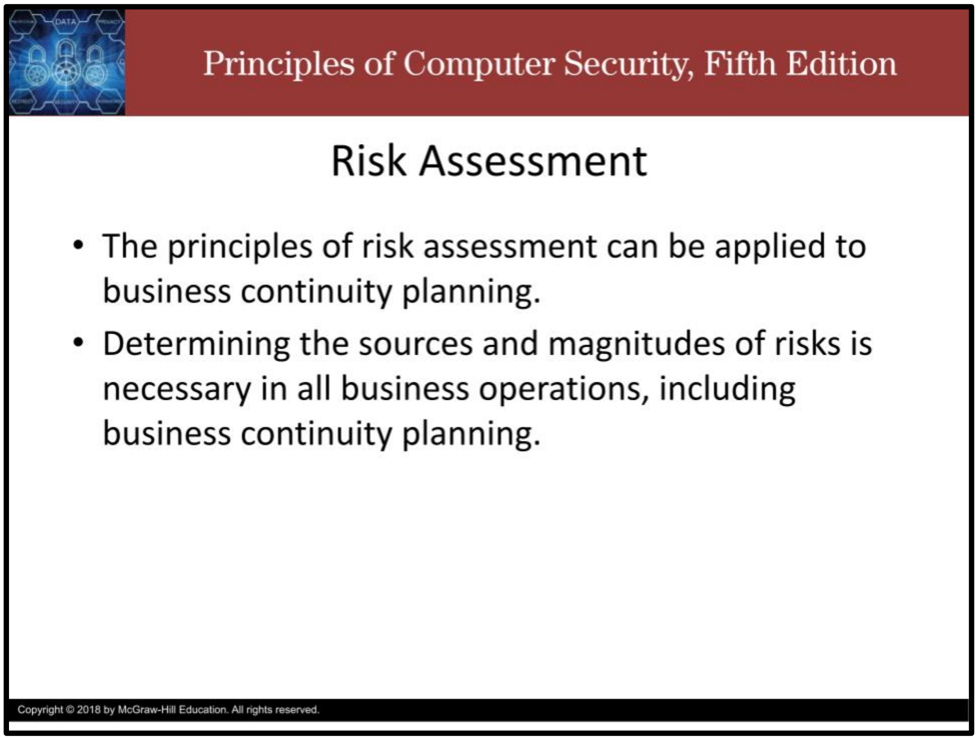
Removing Single Points of Failure

- A key security methodology is to attempt to avoid a single point of failure in critical functions within an organization.
  - When developing your BCP, you should be on the lookout for areas in which a critical function relies on a single item that if lost would stop this critical function.
  - When these points are identified, think about how each of these possible single points of failure can be eliminated (or mitigated).
  - Consider the many resources external to your organization that can impact the operation of your business.

A key security methodology is to attempt to avoid a single point of failure in critical functions within an organization. You should be thinking right now about the principles of separation of duties and least common mechanism. When developing your BCP, you should be on the lookout for areas in which a critical function relies on a single item that, if lost, would stop this critical function. When these points are identified, think about how each of these possible single points of failure can be eliminated or mitigated.

You must also consider the many resources external to your organization that can impact the operation of your business, such as critical infrastructure, like an aging and neglected power grid that could fail at any moment leaving millions without power for months. Maybe a single point of failure lives in the Governor's mansion.

Slide 8



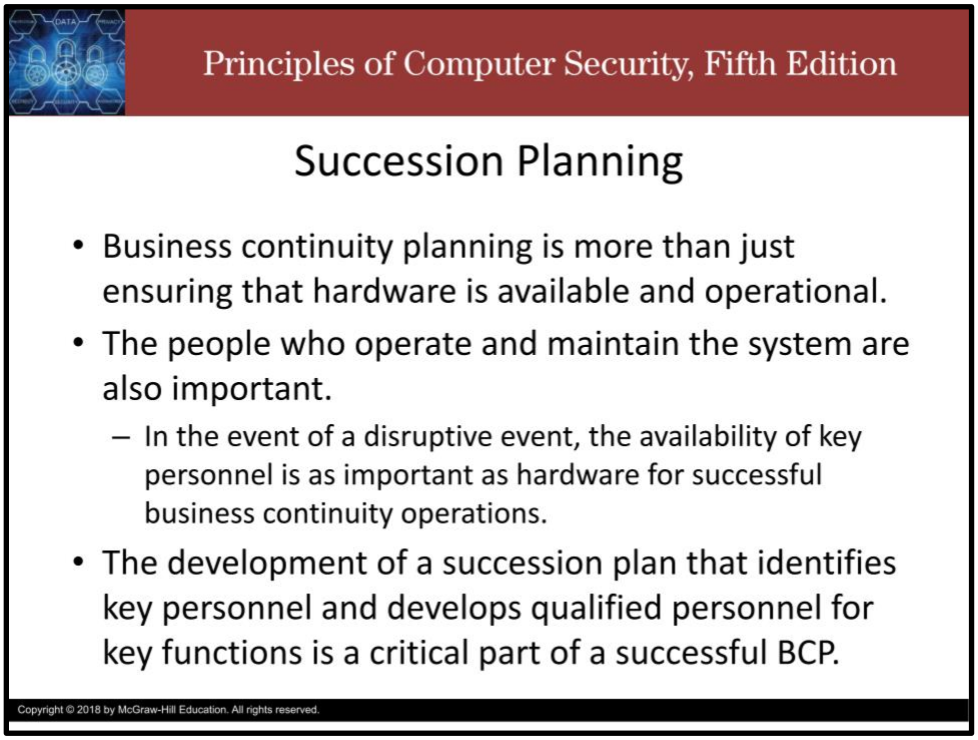
Principles of Computer Security, Fifth Edition

Risk Assessment

- The principles of risk assessment can be applied to business continuity planning.
- Determining the sources and magnitudes of risks is necessary in all business operations, including business continuity planning.

Obviously, the principles of risk assessment can and should be applied to business continuity planning. Determining the sources and magnitudes of risks is necessary in all business operations, which necessarily includes business continuity planning.

Slide 9



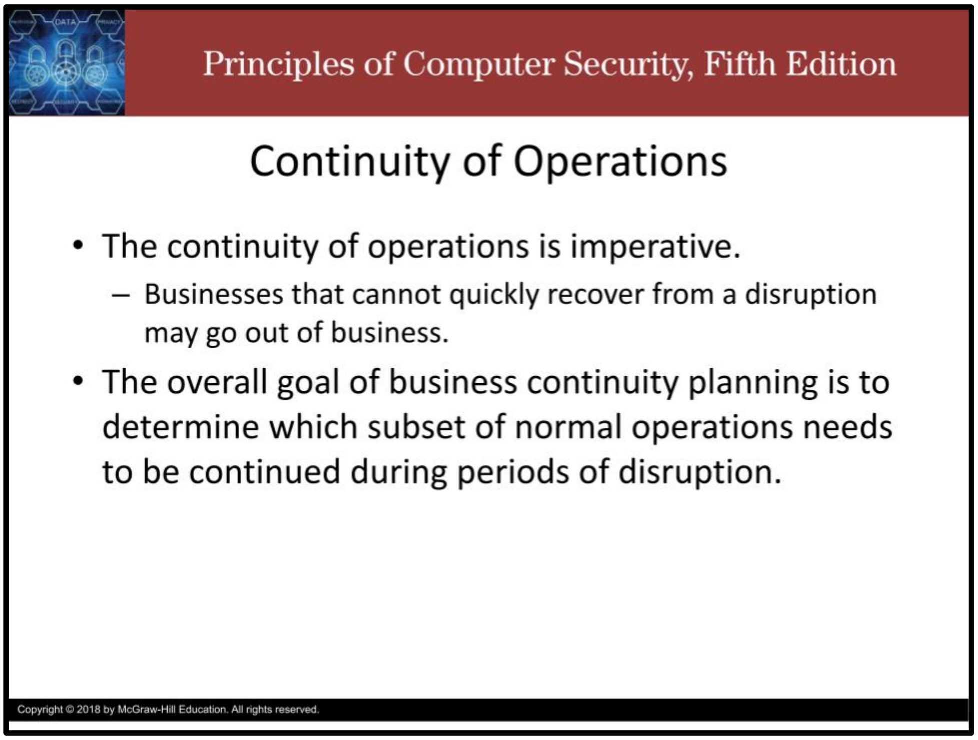
Principles of Computer Security, Fifth Edition

Succession Planning

- Business continuity planning is more than just ensuring that hardware is available and operational.
- The people who operate and maintain the system are also important.
  - In the event of a disruptive event, the availability of key personnel is as important as hardware for successful business continuity operations.
- The development of a succession plan that identifies key personnel and develops qualified personnel for key functions is a critical part of a successful BCP.

Business continuity planning is more than just ensuring that hardware is available and operational.
The people who operate and maintain the system are also important.
In the event of a disruptive event, the availability of key personnel is just as important as the availability of the hardware for successful business continuity operations.
The development of a succession plan that identifies key personnel and develops qualified personnel for key functions is a critical part of a successful BCP.

Slide 10



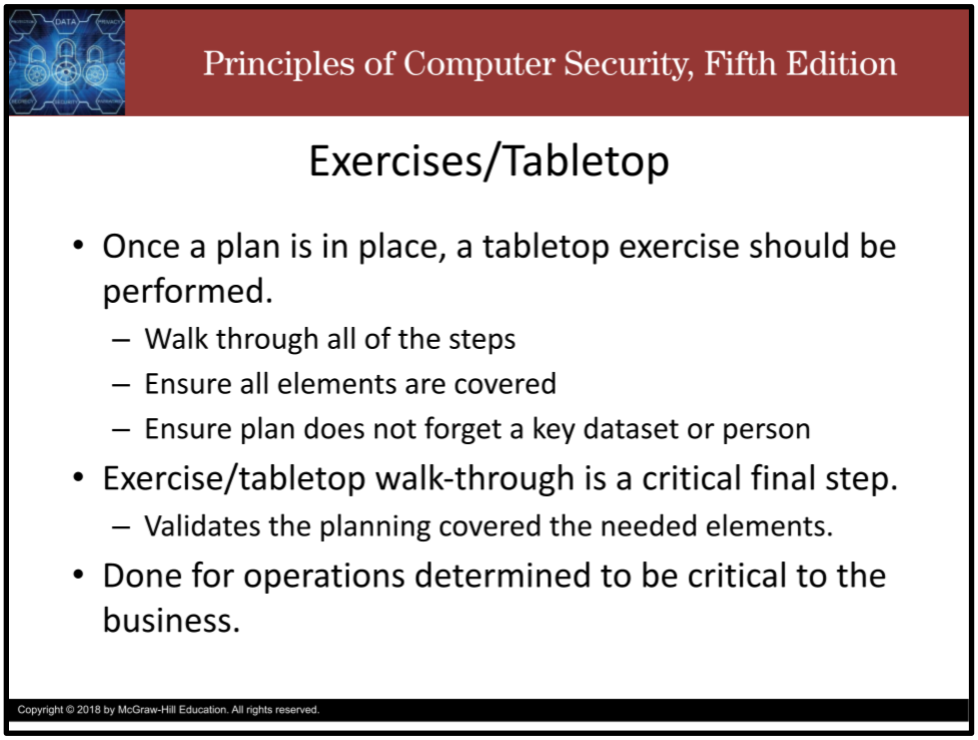
Principles of Computer Security, Fifth Edition

Continuity of Operations

- The continuity of operations is imperative.
  - Businesses that cannot quickly recover from a disruption may go out of business.
- The overall goal of business continuity planning is to determine which subset of normal operations needs to be continued during periods of disruption.

For many businesses, the continuity of operations is imperative.
Businesses that cannot quickly recover from a disruption have a real chance of never recovering.
The overall goal of business continuity planning is to determine which subset of normal operations needs to be continued during periods of disruption.

Slide 11



Principles of Computer Security, Fifth Edition

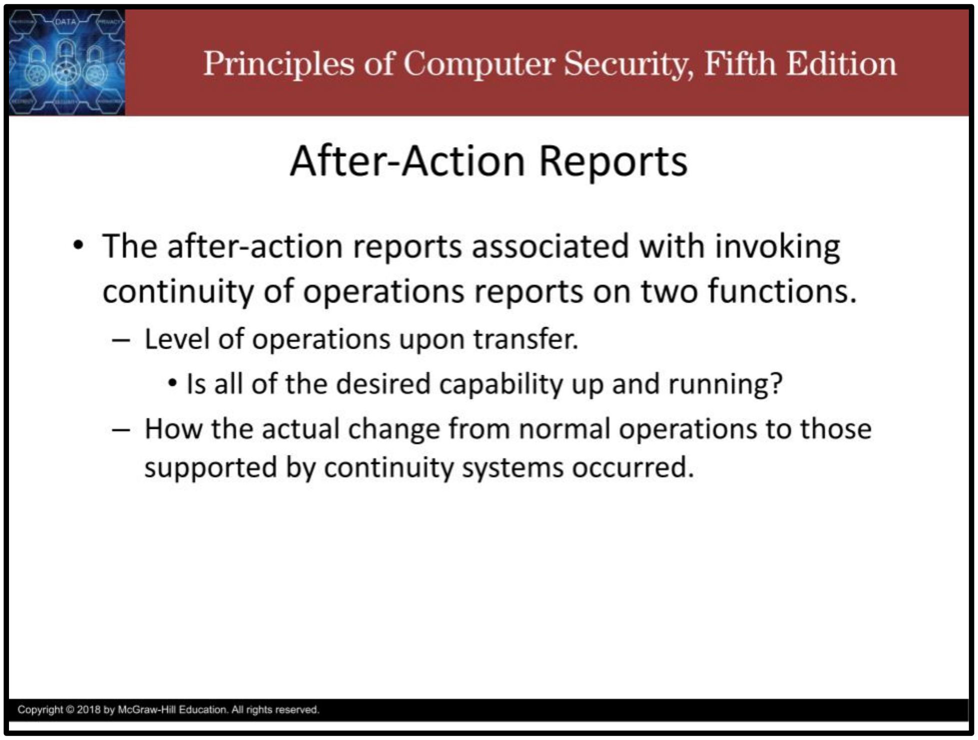
Exercises/Tabletop

- Once a plan is in place, a tabletop exercise should be performed.
  - Walk through all of the steps
  - Ensure all elements are covered
  - Ensure plan does not forget a key dataset or person
- Exercise/tabletop walk-through is a critical final step.
  - Validates the planning covered the needed elements.
- Done for operations determined to be critical to the business.

Once a plan is in place, a tabletop exercise should be performed to walk through all of the steps and ensure that all elements are covered and that the plan does not forget a key dataset or person.
This exercise is a critical final step because it validates that the planning covered the necessary elements.

If this seems like overkill, or cringe, because role-playing games are for dorks, right…. Wrong! This is important because these operations are critical to the business.
The business can't afford to have leadership who are too cool to be prepared.

Slide 12



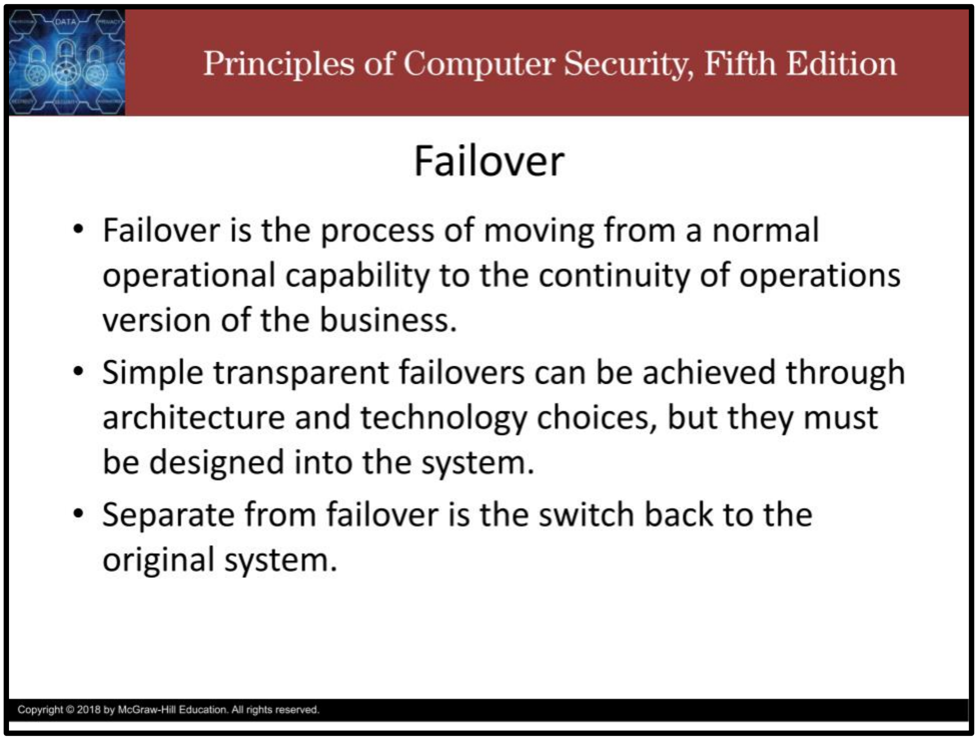
Principles of Computer Security, Fifth Edition

After-Action Reports

- The after-action reports associated with invoking continuity of operations reports on two functions.
  - Level of operations upon transfer.
    - Is all of the desired capability up and running?
  - How the actual change from normal operations to those supported by continuity systems occurred.

The after-action reports associated with invoking continuity of operations discuss two functions:
First is the level of operations upon transfer. Is all of the desired capability up and running?
The second question addresses how the actual change from normal operations to those supported by continuity systems occurred.

Slide 13



Principles of Computer Security, Fifth Edition

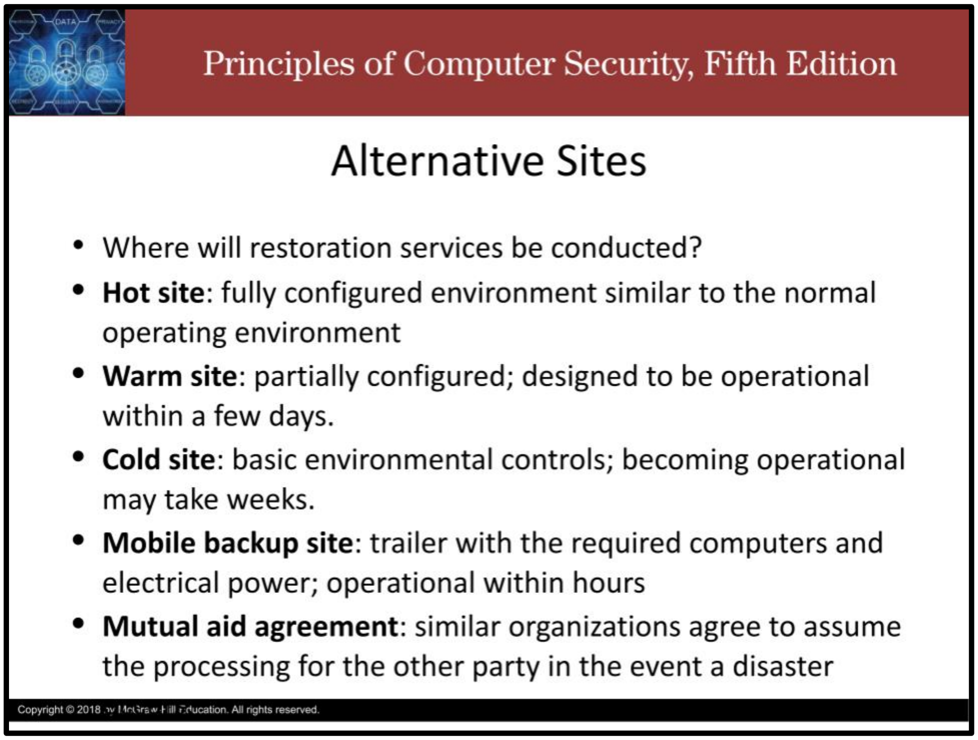
Failover

- Failover is the process of moving from a normal operational capability to the continuity of operations version of the business.
- Simple transparent failovers can be achieved through architecture and technology choices, but they must be designed into the system.
- Separate from failover is the switch back to the original system.

Failover is the process of moving from a normal operational capability to the continuity of operations version of the business. Simple transparent failovers can be achieved through choices of architecture and technology, but they must be designed into the system. Separate from failover is the switch back to the original system.

Once a system is fixed, there needs to be a process for returning the system to normal operations (or switching back to the original system from the backup system). This “failback” mechanism is harder to perform, but it can be performed at a time of the organization’s choosing, as opposed to the initial shift from normal to continuity operations.

Slide 14



Principles of Computer Security, Fifth Edition

Alternative Sites

- Where will restoration services be conducted?
- **Hot site**: fully configured environment similar to the normal operating environment
- **Warm site**: partially configured; designed to be operational within a few days.
- **Cold site**: basic environmental controls; becoming operational may take weeks.
- **Mobile backup site**: trailer with the required computers and electrical power; operational within hours
- **Mutual aid agreement**: similar organizations agree to assume the processing for the other party in the event a disaster

An issue related to the location of backup storage is where the restoration services will be conducted. Determination of when or if an alternative site is needed should be included in recovery and continuity plans. If the organization has suffered physical damage to a facility, having offsite storage of data is only part of the solution. This data will need to be processed somewhere, which means that computing facilities similar to those used in normal operations are required. There are a number of ways to approach this problem, including **hot sites**, **warm sites**, **cold sites**, and mobile backup sites.

A **hot site** is a fully configured environment that is similar to the normal operating environment.
The site can be operational immediately or within a few hours, depending on its configuration and the needs of the organization.

A **warm site** is partially configured, usually having the peripherals and software but perhaps not the more expensive main processing computer.
It is designed to be operational within a few days.

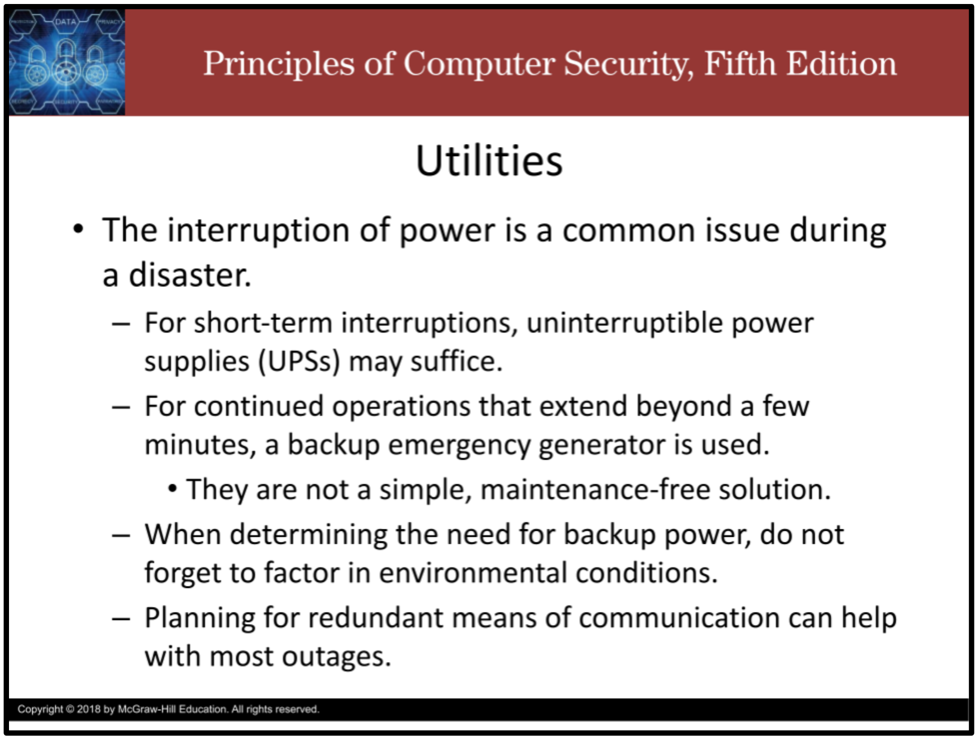
A **cold site** has the basic environmental controls necessary to operate but has few of the computing components necessary for processing.
Getting a cold site operational may take weeks.

A mobile backup site generally is a trailer with the required computers and electrical power.
It can be driven to a location within hours of a disaster and set up to commence processing immediately.

Shared alternate sites may also be considered. With **a mutual aid agreement**, similar organizations agree to assume the processing for the other party in the event a disaster occurs.
This is sometimes referred to as a reciprocal site.

Both shared sites and mutual aid agreements hope that a disaster only affects one of the organizations and spares the other. If not, if both are hit at the same time, then the shared site or mutual aid may be insufficient or unavailable.
On top of that, data security needs to be considered in all cases, especially when sharing infrastructure during an emergency.

Slide 15



Principles of Computer Security, Fifth Edition

Utilities

- The interruption of power is a common issue during a disaster.
  - For short-term interruptions, uninterruptible power supplies (UPSs) may suffice.
  - For continued operations that extend beyond a few minutes, a backup emergency generator is used.
    - They are not a simple, maintenance-free solution.
  - When determining the need for backup power, do not forget to factor in environmental conditions.
  - Planning for redundant means of communication can help with most outages.

Computers and networks obviously require power to operate, so emergency power must be available in the event of any disruption of operations. For short-term interruptions, such as what might occur as the result of an electrical storm, uninterruptible power supplies (UPSs) may suffice. These devices contain a battery that provides steady power for short periods of time—enough to keep a system running should power only be lost for a few minutes, enough time to allow administrators to gracefully halt the system or network. For continued operations that extend beyond a few minutes, another source of power will be required. Generally this is provided by a backup emergency generator.

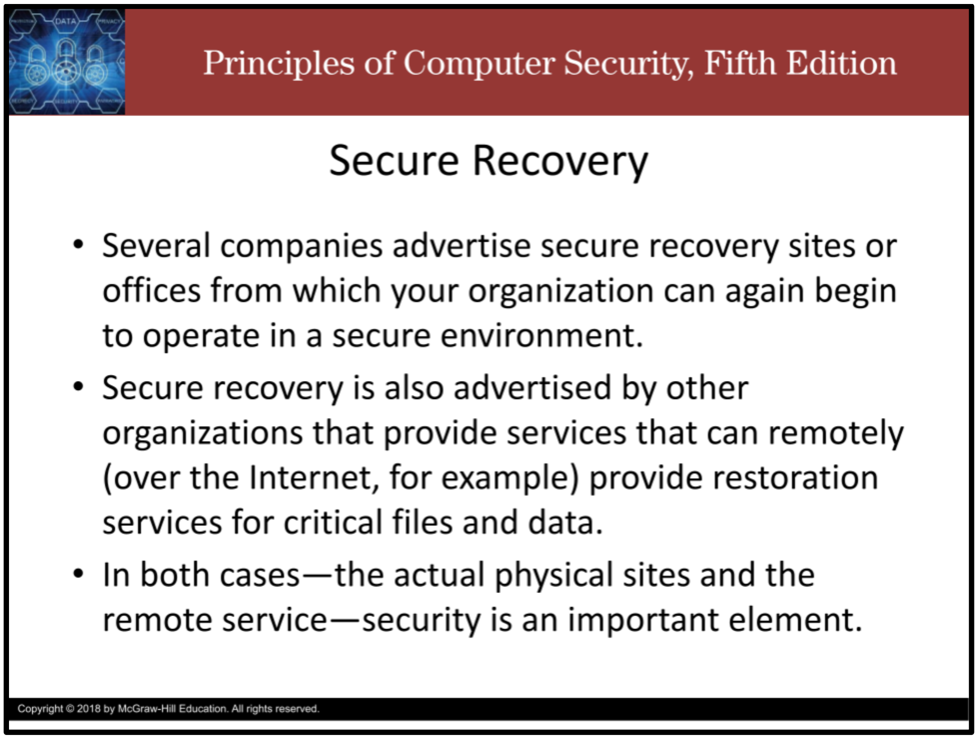
While backup generators are frequently used to provide power during an emergency, they are not a simple, maintenance-free solution. Generators need to be tested on a regular basis, and they can easily become strained if they are required to power too much equipment. If your organization is going to rely on an emergency generator for backup power, you must ensure that the system has reserve capacity beyond the anticipated load for the unanticipated loads that will undoubtedly be placed on it.

Generators also take time to start up, so power to your organization will most likely be lost, even if only briefly, until the generators kick in. This means that you should also use a UPS to allow for a smooth transition to backup power. Generators are also expensive and require fuel—when looking for a place to locate your generator, don’t forget the need to deliver fuel to it or you may find yourself hauling cans of fuel up a number of stairs.

When determining the need for backup power, don’t forget to factor in environmental conditions. Running computer systems in a room with no air conditioning in the middle of the summer can result in an extremely uncomfortable environment for all to work in. Mobile backup sites, generally using trailers, often rely on generators for their power but also factor in the requirement for environmental controls.

Power is not the only essential utility for operations. Depending on the type of disaster that has occurred, telephone and Internet communication may also be lost, and wireless services may not be available. Planning for redundant means of communication (such as using both land lines and wireless) can help with most outages, but for large disasters, your backup plans should include the option to continue operations from a completely different location while waiting for communications in your area to be restored. Telecommunication carriers have their own emergency equipment and are fairly efficient at restoring communications, but it may take a few days.

Slide 16



Principles of Computer Security, Fifth Edition

Secure Recovery

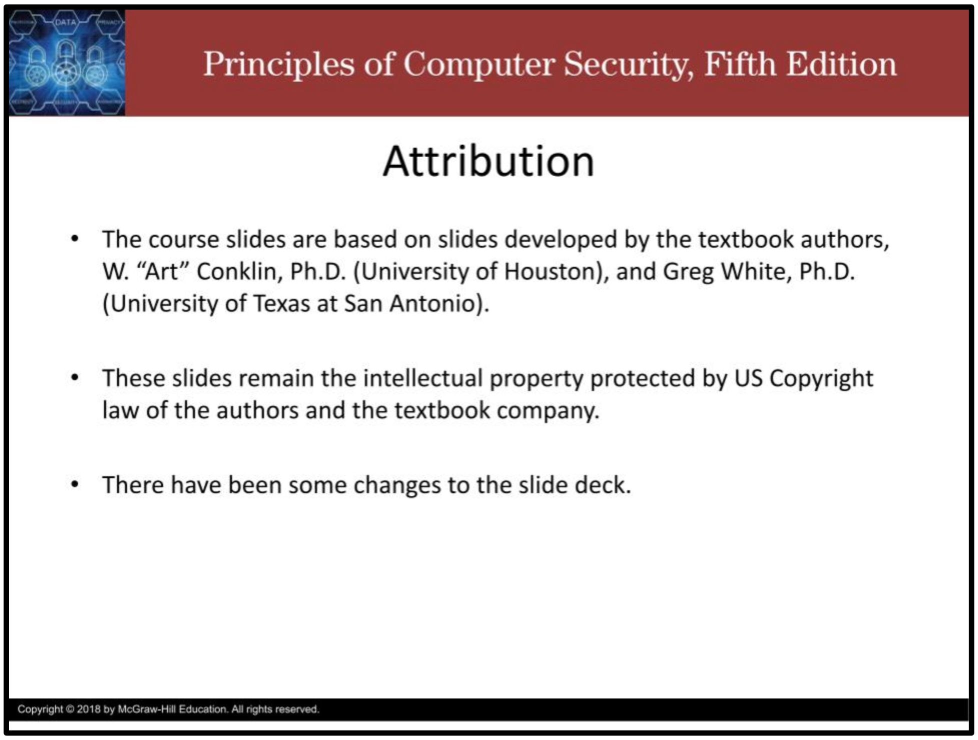
- Several companies advertise secure recovery sites or offices from which your organization can again begin to operate in a secure environment.
- Secure recovery is also advertised by other organizations that provide services that can remotely (over the Internet, for example) provide restoration services for critical files and data.
- In both cases—the actual physical sites and the remote service—security is an important element.

Several companies offer recovery services, including power, communications, and technical support that your organization may need if its operations are disrupted. These companies advertise secure recovery sites or offices from which your organization can again begin to operate in a secure environment. Secure recovery is also advertised by other organizations that provide services that can provide restoration services for critical files and data.

In both cases—the actual physical sites and the remote service—security is an important element. During a disaster, your data does not become any less important, and you will want to make sure that you maintain the security (in terms of confidentiality and integrity, for example) of your data.

As in other aspects of security, the decision to employ these services should be made based on a calculation of the benefits weighed against the potential loss if alternative means are used.

Slide 17



Principles of Computer Security, Fifth Edition

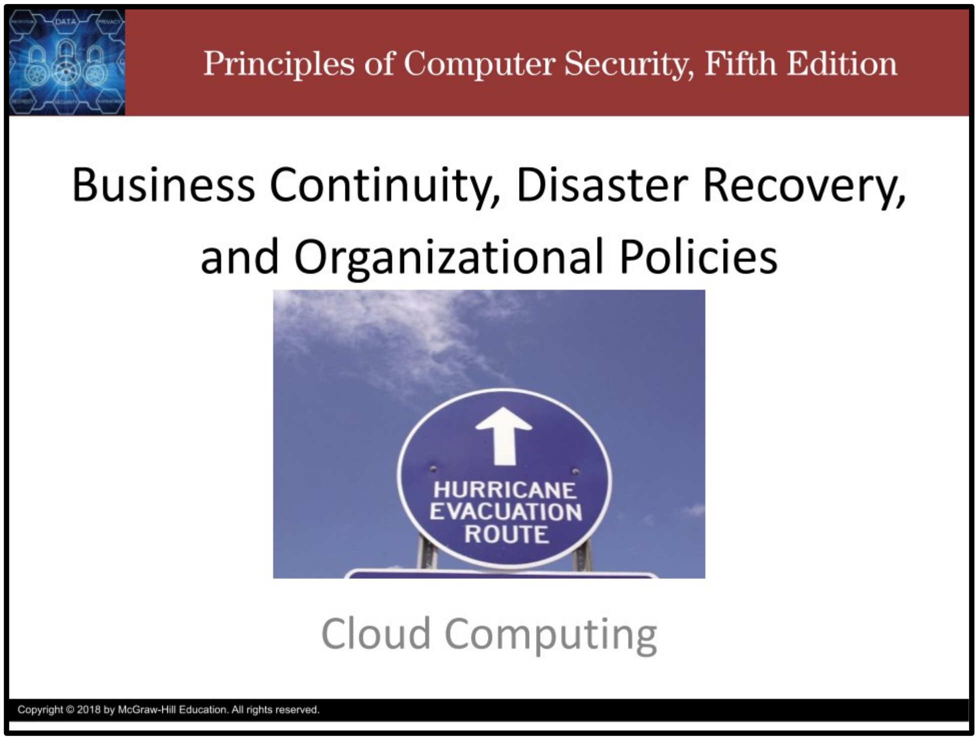
Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Thank you and take care.

Business Continuity, Disaster Recovery, and Organizational Policies: Cloud Computing

Slide 1



Principles of Computer Security, Fifth Edition

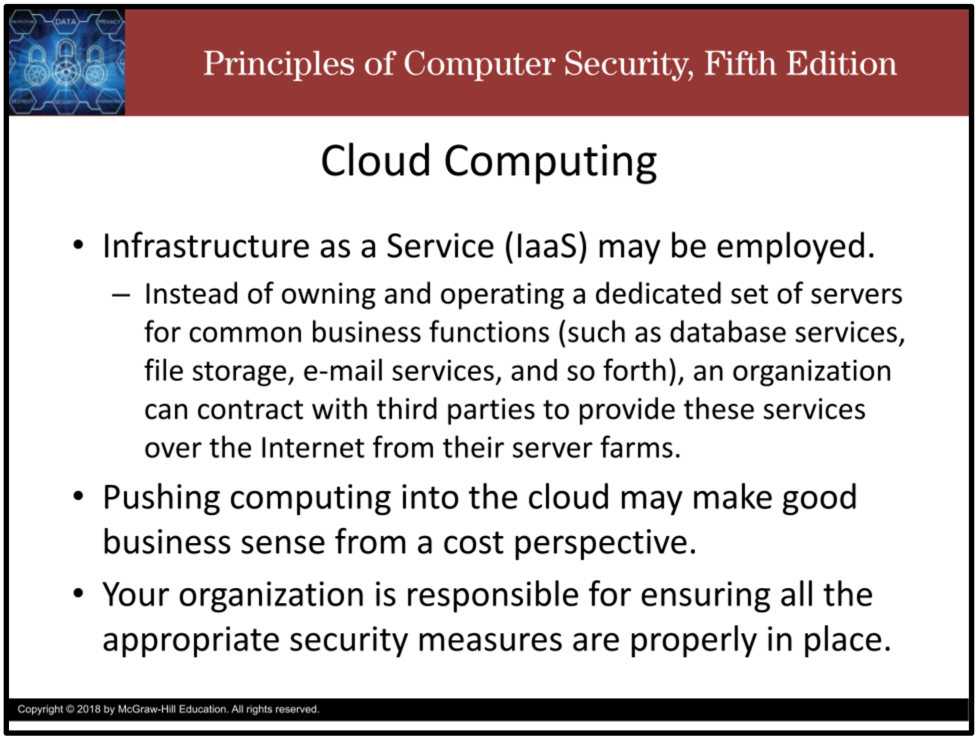
Business Continuity, Disaster Recovery, and Organizational Policies

HURRICANE
EVACUATION
ROUTE

Cloud Computing

Howdy! In this video, we mention cloud computing in the context of business continuity and disaster recovery.

Slide 2



Principles of Computer Security, Fifth Edition

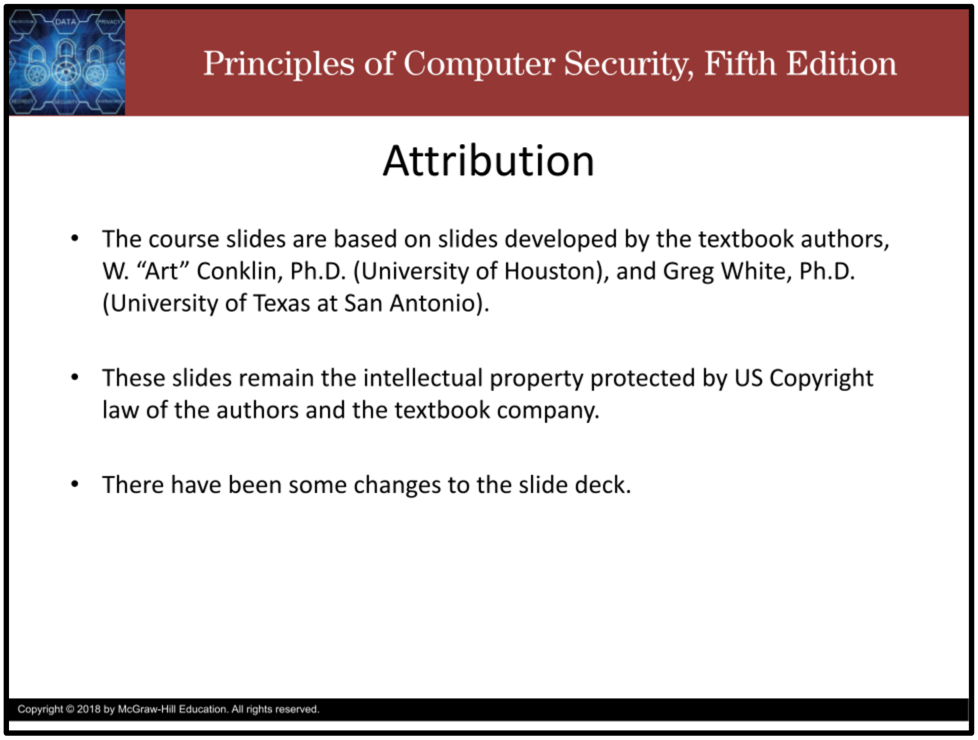
Cloud Computing

- Infrastructure as a Service (IaaS) may be employed.
  - Instead of owning and operating a dedicated set of servers for common business functions (such as database services, file storage, e-mail services, and so forth), an organization can contract with third parties to provide these services over the Internet from their server farms.
- Pushing computing into the cloud may make good business sense from a cost perspective.
- Your organization is responsible for ensuring all the appropriate security measures are properly in place.

One of the most powerful innovations to computing via the Internet is the concept of cloud computing. Instead of owning and operating a dedicated set of servers for common business functions such as database services, file storage, e-mail services, and so forth, an organization can contract with third parties to provide these services over the Internet from their server farms. This is commonly referred to as Infrastructure as a Service (IaaS). The concept is that operations and maintenance is an activity that has become a commodity, and the Internet provides a reliable mechanism to access this more economical form of operational computing.

Pushing computing into the cloud may make good business sense from a cost perspective, but doing so does not change the fact that your organization is still responsible for ensuring that all the appropriate security measures are properly in place. How are backups being performed? What plan is in place for disaster recovery? How frequently are systems patched? What is the service level agreement (SLA) associated with the systems? It is easy to ignore the details when outsourcing these critical yet costly elements, but when something bad occurs, you must have confidence that the appropriate level of protections has been applied. These are the serious questions and difficult issues to resolve when moving computing into the cloud—location may change, but responsibility and technical issues remain (or may be created).

Slide 3



Principles of Computer Security, Fifth Edition

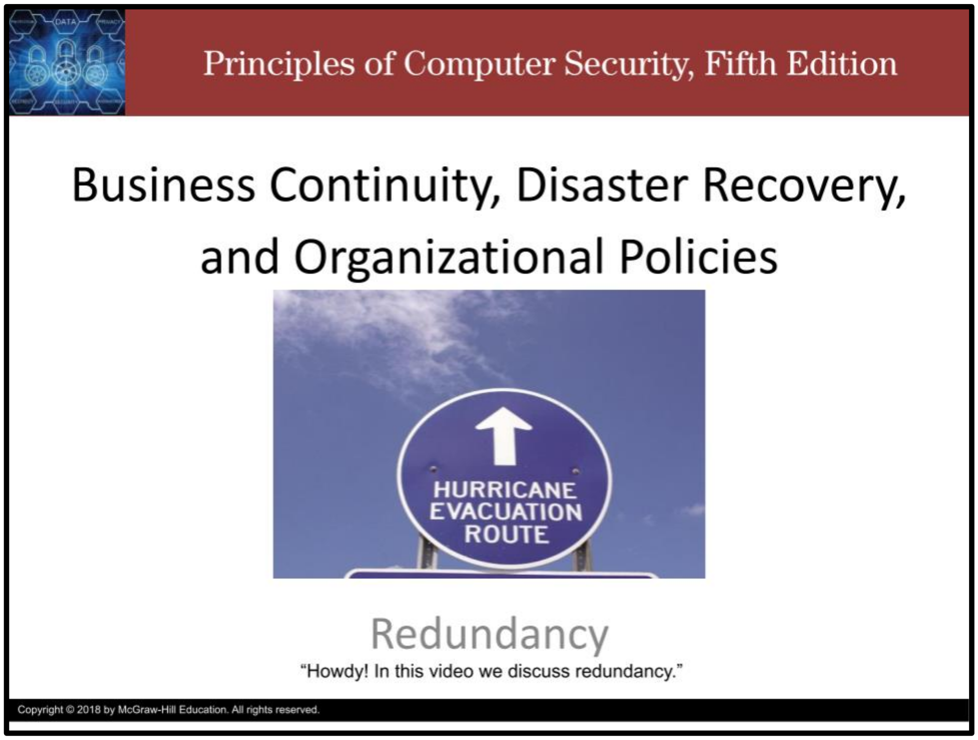
Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Thank you and take care.

Business Continuity, Disaster Recovery, and Organizational Policies: Redundancy

Slide 1



Principles of Computer Security, Fifth Edition

Business Continuity, Disaster Recovery, and Organizational Policies

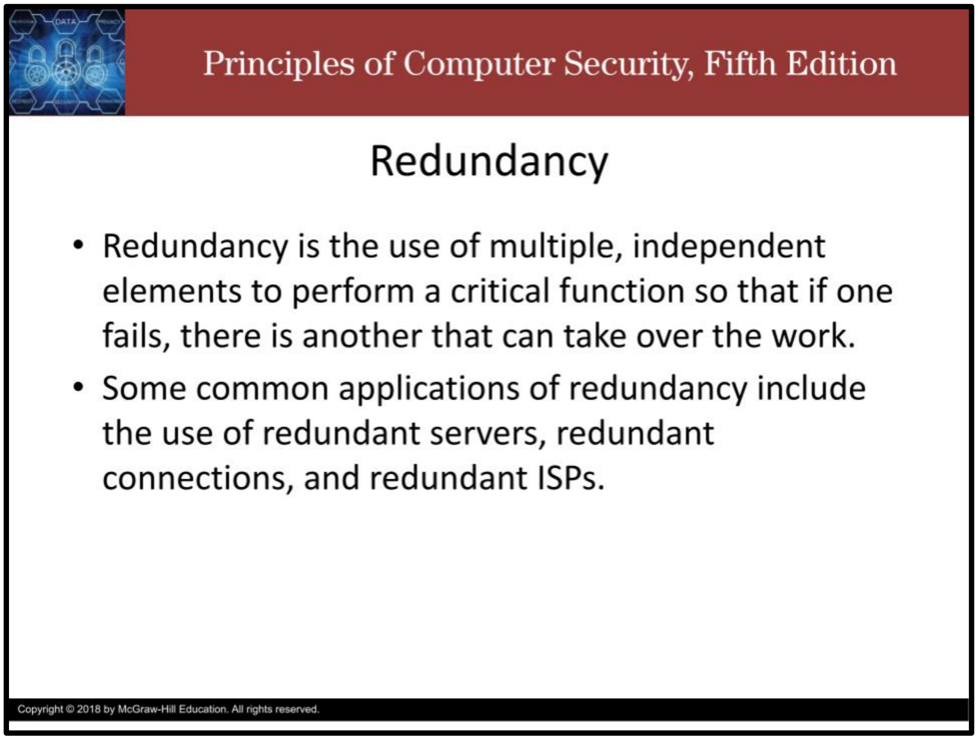
HURRICANE
EVACUATION
ROUTE

Redundancy

“Howdy! In this video we discuss redundancy.”

Howdy! In this video we discuss redundancy.

Slide 2



Principles of Computer Security, Fifth Edition

Redundancy

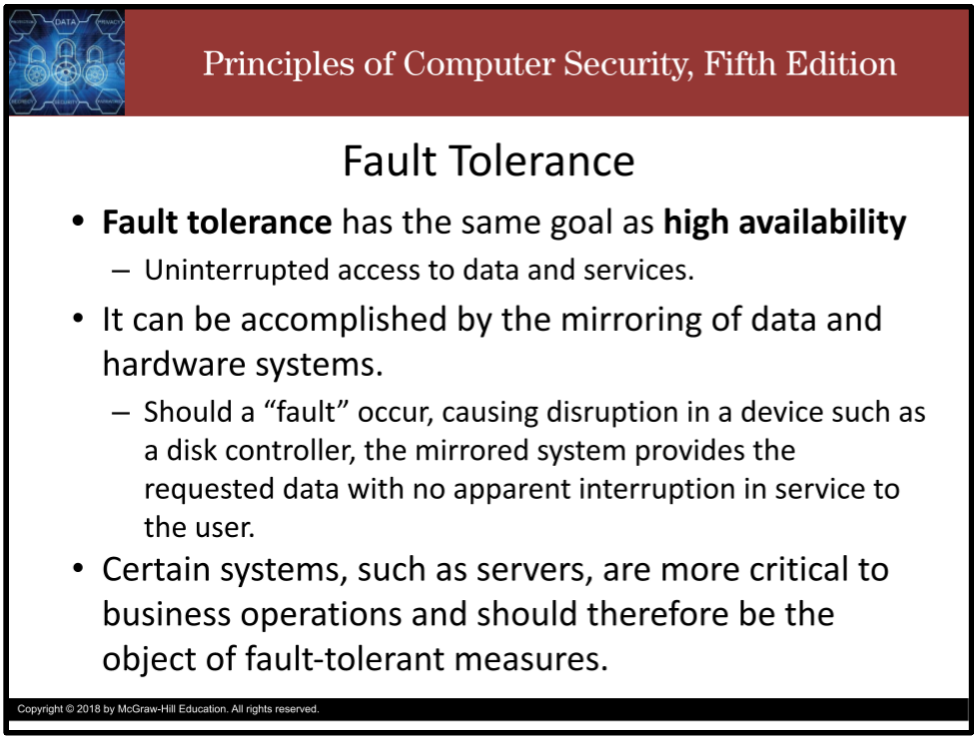
- Redundancy is the use of multiple, independent elements to perform a critical function so that if one fails, there is another that can take over the work.
- Some common applications of redundancy include the use of redundant servers, redundant connections, and redundant ISPs.

Redundancy is the use of multiple, independent elements to perform a critical function so that if one fails, there is another that can take over the work.

When developing business continuity or disaster recovery plans, you should consider measures involving redundancy and spare parts.

Some common applications of redundancy include the use of redundant servers, redundant connections, and redundant ISPs.

Slide 3



Principles of Computer Security, Fifth Edition

Fault Tolerance

- **Fault tolerance** has the same goal as **high availability**
  - Uninterrupted access to data and services.
- It can be accomplished by the mirroring of data and hardware systems.
  - Should a “fault” occur, causing disruption in a device such as a disk controller, the mirrored system provides the requested data with no apparent interruption in service to the user.
- Certain systems, such as servers, are more critical to business operations and should therefore be the object of fault-tolerant measures.

Some other terms that may be used in discussions of continuity of operations in the face of a disruption of some sort are high availability and fault tolerance.

One of the objectives of security is the availability of data and processing power when an authorized user desires it.

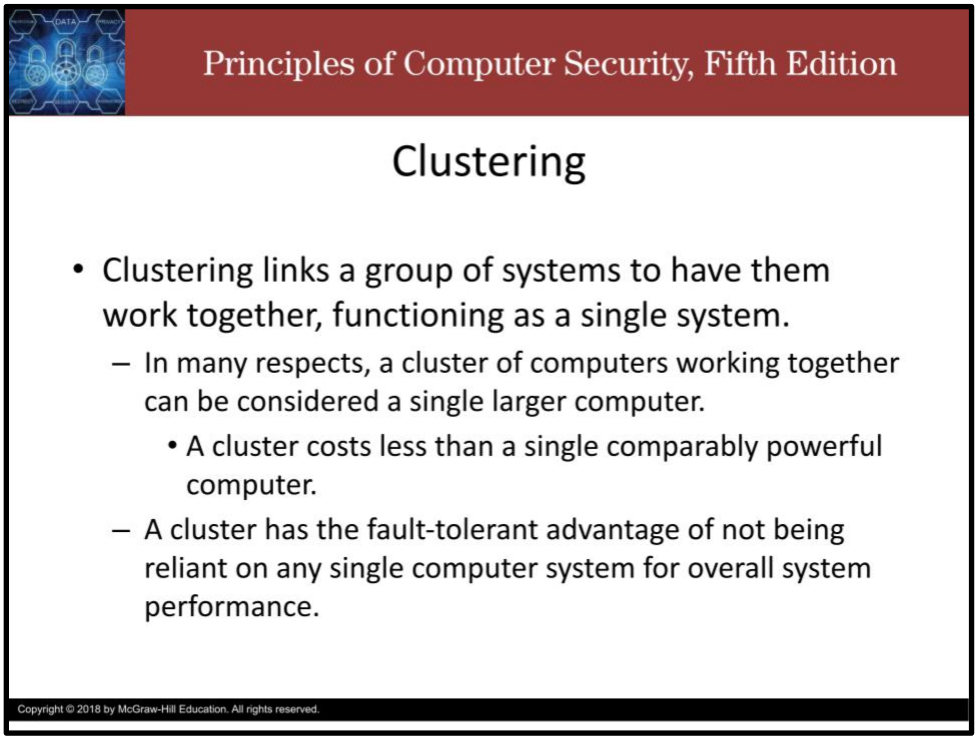
High availability refers to the ability to maintain availability of data and operational processing despite a disrupting event.

Generally this requires redundant systems, in terms of both power and processing, so that should one system fail, the other can take over operations without any break in service. High availability is more than data redundancy; it requires that both data and services be available.

Fault tolerance basically has the same goal as high availability—the uninterrupted access to data and services—and is accomplished by the mirroring of data and systems. Should a “fault” occur, causing disruption in a device such as a disk controller, the mirrored system provides the requested data with no apparent interruption in service to the user.

High availability clustering is another method used to provide redundancy in critical situations. These clusters consist of additional computers upon which a critical process can be started if the cluster detects that there has been a hardware or software problem on the main system. Certain systems, such as servers, are more critical to business operations and should, therefore, be the object of fault-tolerance measures. A common technique used in fault tolerance is load balancing. Another closely related technique is clustering. Providing redundant systems and equipment comes with a price, and the costs and benefits of providing this level of continuous, uninterrupted operation need to be understood and weighed carefully.

Slide 4



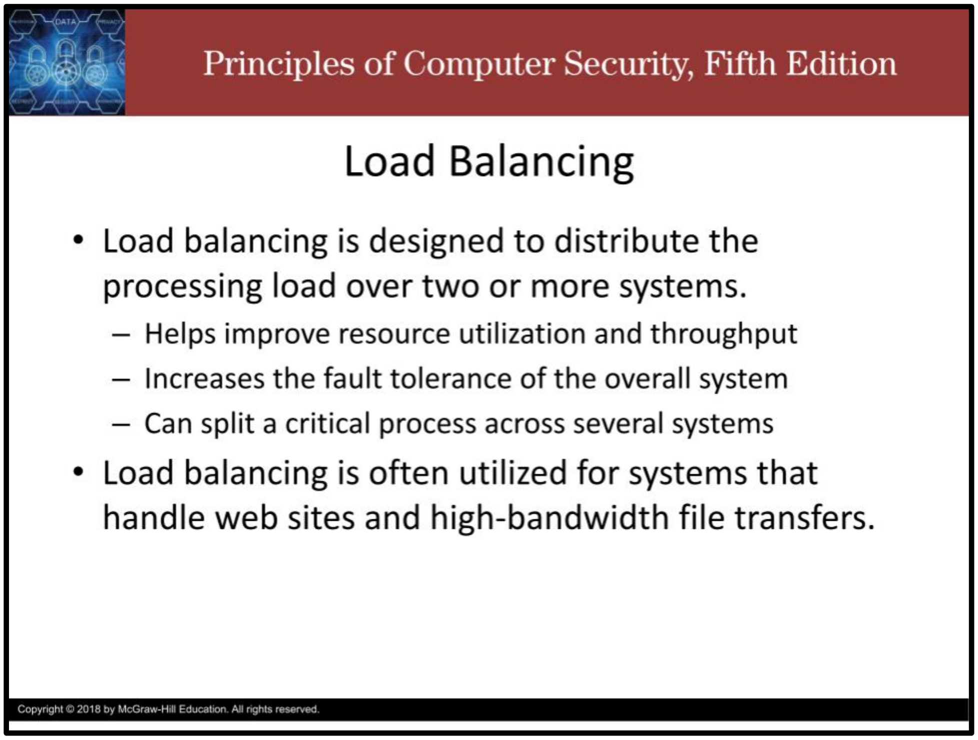
Principles of Computer Security, Fifth Edition

Clustering

- Clustering links a group of systems to have them work together, functioning as a single system.
  - In many respects, a cluster of computers working together can be considered a single larger computer.
    - A cluster costs less than a single comparably powerful computer.
  - A cluster has the fault-tolerant advantage of not being reliant on any single computer system for overall system performance.

Clustering links a group of systems together to have them function as a single system.
In many respects, a cluster of computers working together can be considered as a single large computer.
One advantage of this approach is that a cluster could cost less than a single comparably powerful computer, depending on the type of performance you need more of.
A cluster also has the fault-tolerant advantage of not being reliant on any single computer system for overall system performance.

Slide 5



Principles of Computer Security, Fifth Edition

Load Balancing

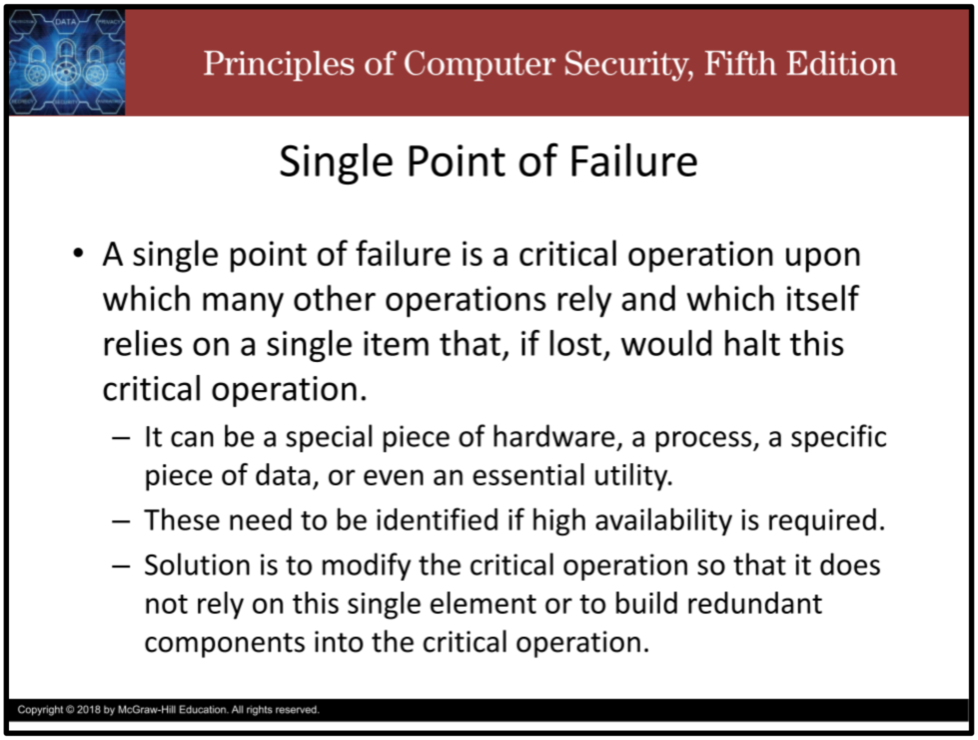
- Load balancing is designed to distribute the processing load over two or more systems.
  - Helps improve resource utilization and throughput
  - Increases the fault tolerance of the overall system
  - Can split a critical process across several systems
- Load balancing is often utilized for systems that handle web sites and high-bandwidth file transfers.

Load balancing is designed to distribute the processing load over two or more systems.

Load balancing helps improve resource utilization and throughput and increases the fault tolerance of the overall system because it can split a critical process across several systems

Load balancing is often utilized for systems that handle web sites and high-bandwidth file transfers.

Slide 6



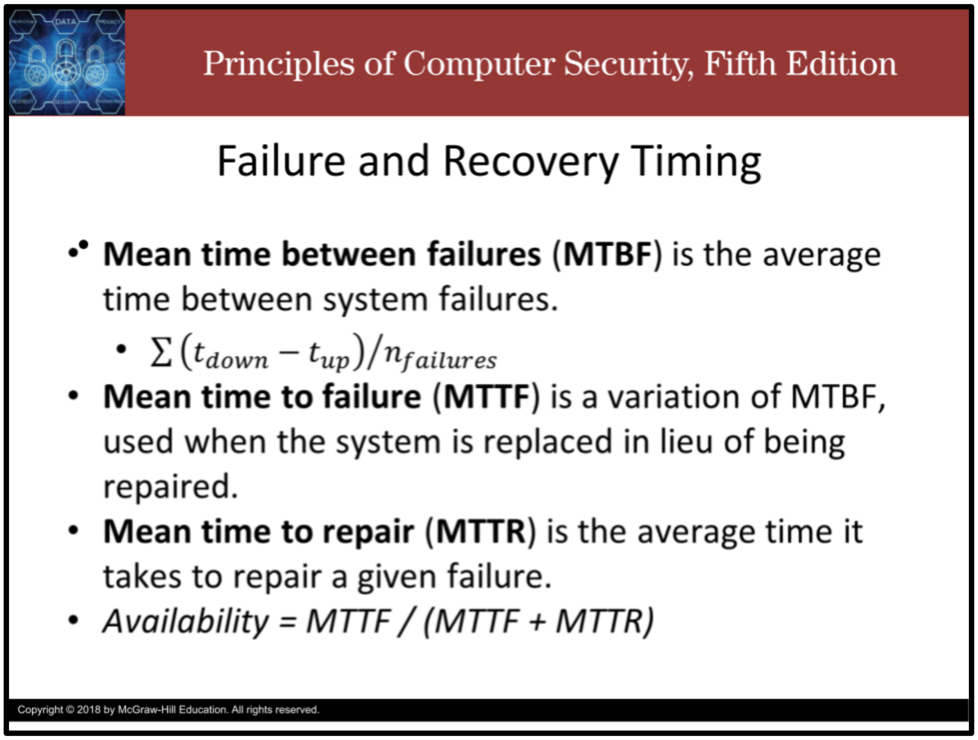
Principles of Computer Security, Fifth Edition

Single Point of Failure

- A single point of failure is a critical operation upon which many other operations rely and which itself relies on a single item that, if lost, would halt this critical operation.
  - It can be a special piece of hardware, a process, a specific piece of data, or even an essential utility.
  - These need to be identified if high availability is required.
  - Solution is to modify the critical operation so that it does not rely on this single element or to build redundant components into the critical operation.

Single points of failure need to be identified if high availability is required because they are potentially the “weak links” in the chain that can cause disruption of the organization’s operations. Generally, the solution to a single point of failure is to modify the critical operation so that it does not rely on this single element or to build redundant components into the critical operation to take over the process should one of these points fail.

Slide 7



Principles of Computer Security, Fifth Edition

Failure and Recovery Timing

- **Mean time between failures** (**MTBF**) is the average time between system failures.
  - $\sum(t_{down} - t_{up})/n_{failures}$
- **Mean time to failure** (**MTTF**) is a variation of MTBF, used when the system is replaced in lieu of being repaired.
- **Mean time to repair** (**MTTR**) is the average time it takes to repair a given failure.
- *Availability = MTTF / (MTTF + MTTR)*

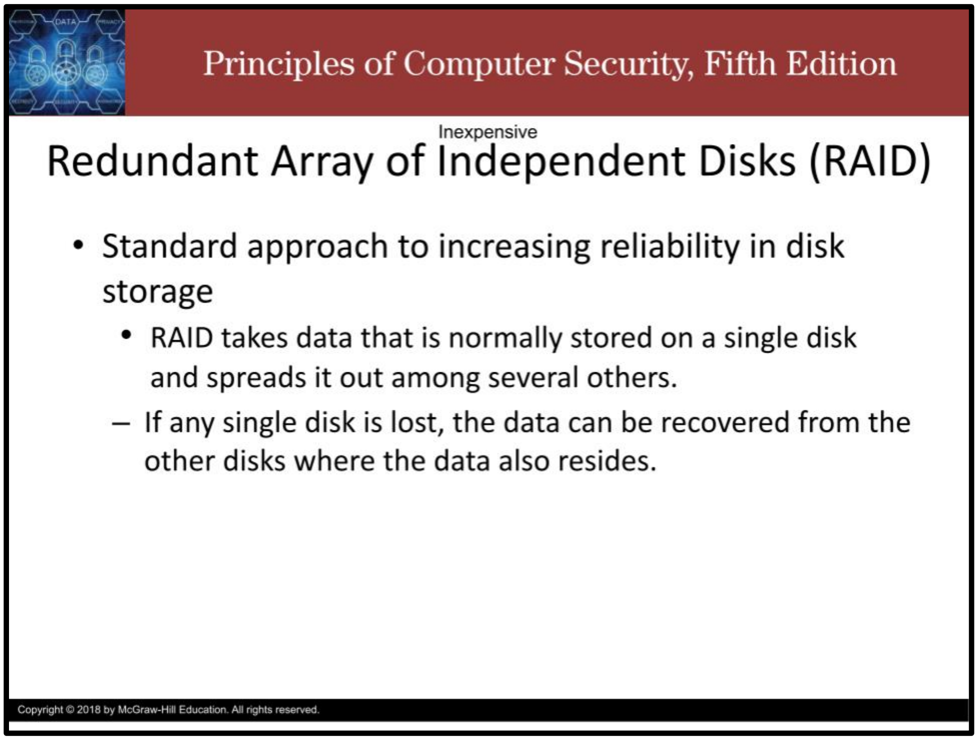
Several important concepts are involved in the issue of fault tolerance and system recovery.
The first is **mean time between failures.**
Mean time between failures (**MTBF**) is a common measure of reliability of a system and is an expression of the average time between system failures.
Mean time to failure (**MTTF**) is a variation of MTBF and is commonly used instead of MTBF when the system is replaced in lieu of being repaired.

A second important concept to understand is **mean time to repair (**or mean time to restore or recovery).
Mean time to repair (**MTTR**) is a common measure of how long it takes to repair a given failure.

This is the average time that it will take to restore a system to operational status or to recover from a failure.

Knowing these times for components of various critical systems is important to developing effective, and realistic, recovery plans, including DRP, BCP, and backup plans.

Slide 8



Principles of Computer Security, Fifth Edition

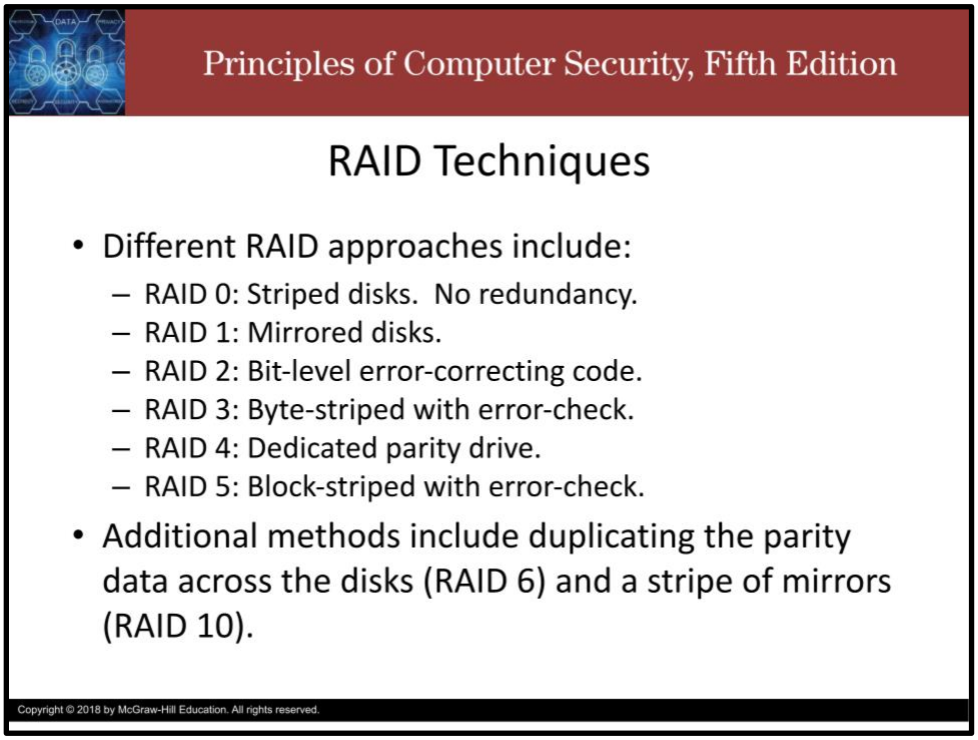
Redundant Array of Inexpensive Independent Disks (RAID)

- Standard approach to increasing reliability in disk storage
  - RAID takes data that is normally stored on a single disk and spreads it out among several others.
  - If any single disk is lost, the data can be recovered from the other disks where the data also resides.

RAID is a popular (if not standard) approach to increasing reliability in disk storage. RAID takes data that is normally stored on a single disk and spreads it out among several others in some way. If any single disk is lost, the data can be recovered from the other disks where the data also resides.

With the price of disk storage decreasing, this approach has become increasingly popular to the point that many individual users even have **RAID** arrays for their home systems. RAID can also increase the speed of data recovery, as multiple drives can be busy retrieving requested data at the same time instead of relying on just one disk to do the work.

Slide 9



Principles of Computer Security, Fifth Edition

RAID Techniques

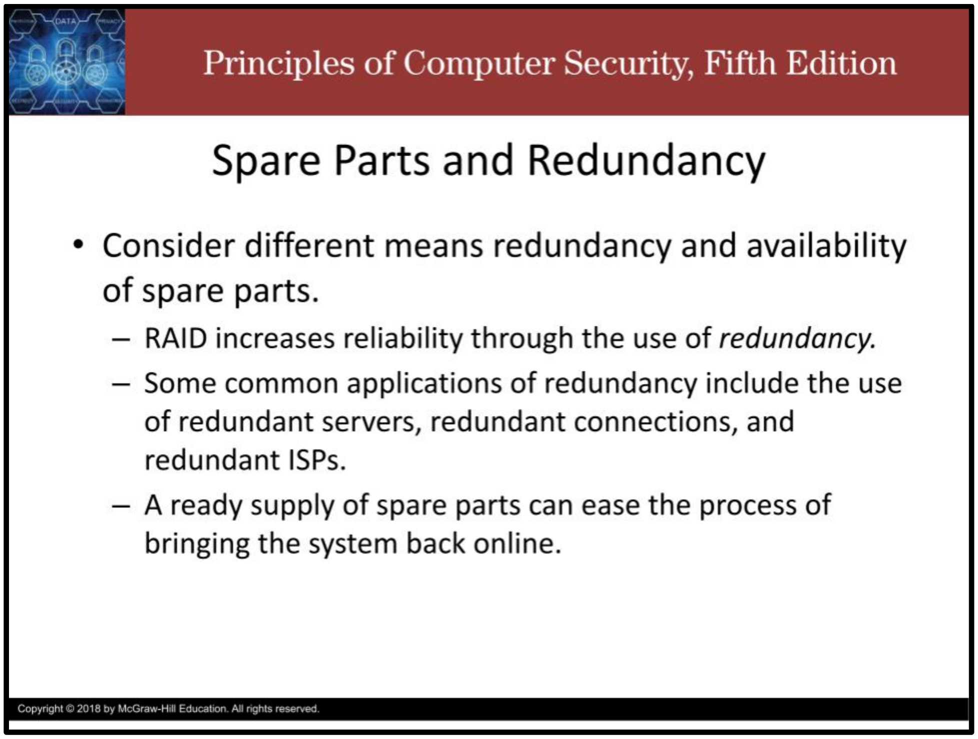
- Different RAID approaches include:
  - RAID 0: Striped disks. No redundancy.
  - RAID 1: Mirrored disks.
  - RAID 2: Bit-level error-correcting code.
  - RAID 3: Byte-striped with error-check.
  - RAID 4: Dedicated parity drive.
  - RAID 5: Block-striped with error-check.
- Additional methods include duplicating the parity data across the disks (RAID 6) and a stripe of mirrors (RAID 10).

Several different RAID approaches can be considered:

RAID 0 (striped disks) simply spreads the data that would be kept on the one disk across several disks. This decreases the time it takes to retrieve data, because the data is read from multiple drives at the same time, but it does not improve reliability, because the loss of any single drive will result in the loss of all the data (since portions of files are spread out among the different disks). With RAID 0, the data is split across all the drives with no redundancy offered.
RAID 1 (mirrored disks) is the opposite of RAID 0. RAID 1 copies the data from one disk onto two or more disks. If any single disk is lost, the data is not lost since it is also copied onto the other disk(s). This method can be used to improve reliability and retrieval speed, but it is relatively expensive when compared to other RAID techniques.
RAID 2 (bit-level error-correcting code) is not typically used, as it stripes data across the drives at the bit level as opposed to the block level. It is designed to be able to recover the loss of any single disk through the use of error-correcting techniques.
RAID 3 (byte-striped with error check) spreads the data across multiple disks at the byte level with one disk dedicated to parity bits. This technique is not commonly implemented, because input/output operations can’t be overlapped due to the need for all to access the same disk (the disk with the parity bits).
RAID 4 (dedicated parity drive) stripes data across several disks but in larger stripes than in RAID 3, and it uses a single drive for parity-based error checking. RAID 4 has the disadvantage of not improving data retrieval speeds, since all retrievals still need to access the single parity drive.
RAID 5 (block-striped with error check) is a commonly used method that stripes the data at the block level and spreads the parity data across the drives. This provides both reliability and increased speed performance. This form requires a minimum of three drives.

RAID 0 through 5 are the original techniques, with RAID 5 being the most common method used, as it provides both the reliability and speed improvements. Additional methods have been implemented, such as duplicating the parity data across the disks (RAID 6) and a stripe of mirrors (RAID 10).

Slide 10



Principles of Computer Security, Fifth Edition

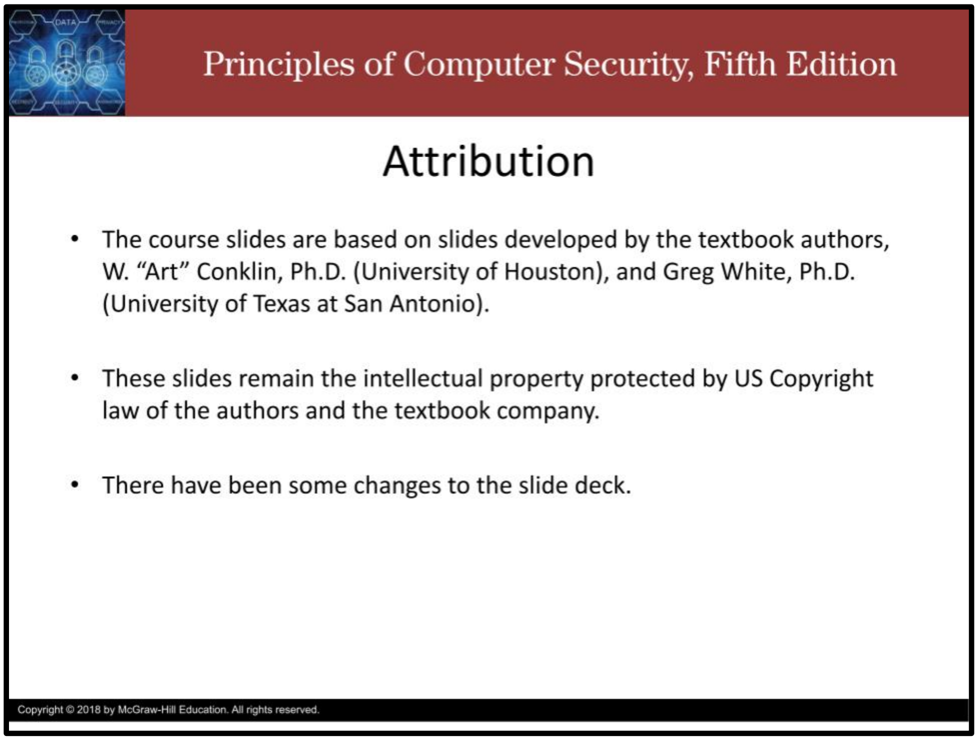
Spare Parts and Redundancy

- Consider different means redundancy and availability of spare parts.
  - RAID increases reliability through the use of *redundancy.*
  - Some common applications of redundancy include the use of redundant servers, redundant connections, and redundant ISPs.
  - A ready supply of spare parts can ease the process of bringing the system back online.

RAID increases reliability through the use of redundancy. When developing plans for ensuring that an organization has what it needs to keep operating, even if hardware or software fails or if security is breached, you should consider other measures involving redundancy and spare parts. Some common applications of redundancy include the use of redundant servers, redundant connections, and redundant ISPs. The need for redundant servers and connections may be fairly obvious, but the need for redundant ISPs may not be so, at least initially. Many ISPs already have multiple accesses to the Internet on their own, but by having additional ISP connections, an organization can reduce the chance that an interruption of one ISP will negatively impact the organization. Ensuring uninterrupted access to the Internet by employees or access to the organization’s e-commerce site for customers is becoming increasingly important.

Many organizations don’t see the need for maintaining a supply of spare parts. After all, with the price of storage dropping and the speed of processors increasing, why replace a broken part with older technology? However, a ready supply of spare parts can ease the process of bringing the system back online. Replacing hardware and software with newer versions can sometimes lead to problems with compatibility. An older version of some piece of critical software may not work with newer hardware, which may be more capable in a variety of ways. Having critical hardware (or software) spares for critical functions in the organization can greatly facilitate maintaining business continuity in the event of software or hardware failures.

Slide 11



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Thank you and take care.