ICSI MODULE 12:

Physical Security

12.1 Physical Security

Physical security is actually a multifaceted topic. The most obvious issue is to physically secure machines, but beyond that you must consider issues such as controlling access to your building and knowing how to respond to fires. Monitoring systems such as alarms and cameras are also a part of physical security.

12.1.1 Equipment Security

Physical security begins with controlling access to the building and to key rooms within the building. At the most basic level, it includes having a locked door on the server room. In addition to that, you must also have some way of controlling who has access to that room.

A highly recommended approach is a swipe card or password key entry system that records who enters the room and when. You should also consider the room itself. It should not have a window, or if it does, it should be a reinforced window and someone outside should not be able to easily view inside the room. The room should also be fireproof, because a fire in the server room would be a significant disaster.

The server room is obviously a key item to secure, but it is not the only item. If routers or switches are distributed in the building, they must be in locations that are not easily accessible by unauthorised personnel. Locked closets make a good location for these items. Locking down workstations so they are secured to the desk is also a common practice. This makes theft of those computers significantly more difficult.

Essentially any device that is itself valuable or contains data that is valuable must be physically secured. Equipping mobile business phones with the ability to remotely wipe them is also becoming common practice. That way if they become stolen or lost, the administrator can remotely wipe all data on the phone.

12.1.2 Securing Building Access

After you have secured the equipment you must also control access to the building itself. A common method is to have a locked door or barrier that requires an employee ID to enter. A sign-in sheet is also a good way to track who enters and exits your office. The level of effort put into securing physical access to the building will vary depending on the organisation's security needs.

A mantrap is an often-used security mechanism in high-security environments. A mantrap consists of two doors with a short hallway between them. The second door cannot open until the first door is closed. This prevents tailgating, which is the process of an unauthorised person following an authorised person through a secure door. This can be further enhanced by having each door use a different authentication method. Perhaps the first door requires a key and the second requires a passcode. This two-factor authentication system would be difficult for an intruder to circumvent.

Other methods of securing building access include the external areas of a building. For example, a parking lot can be designed so that a person must make turns every 50 feet or so to exit. This prevents a thief or intruder from "speeding away" and makes it more likely that someone will be able to note their license plate, or that even police might arrive before they escape.

Fences are also important. Having some level of fencing is essential. High-security environments might use a tall fence, even topped with concertina wire. This might not be appropriate for many organisations, but even a decorative hedgerow provides some level of barrier to slow down intruders.

Lighting is also important. Intruders usually prefer to enter in the dark to reduce the chance of being noticed or even caught. A well-lighted external building impedes intruders' intentions to enter surreptitiously. Furthermore, internal lighting can also be helpful. You probably notice that many retail stores leave the store lights on after closing. This allows passing police officers to easily see whether someone is in the building.

12.1.3 Monitoring

Video monitoring is becoming more affordable and more sophisticated. High-definition video cameras, including cameras with night vision capability, are now fairly inexpensive. Retail stores often find that by placing cameras in highly visible areas, the incidence of theft declines. Stoplights equipped with cameras usually reduce the number of people who run red lights.

Placing cameras in or around your facility requires a little bit of thought. First and foremost, the cameras must be placed so that they have an unobstructed view of the areas you want to monitor. At a minimum, all entrances and exits should have camera monitoring.

You might also want cameras in main internal hallways, just outside critical areas (that is, server rooms), and possibly around the perimeter of your building. The cameras also need to be placed so that they are not easily disabled by an intruder. This usually means placing them at a height that is difficult for someone to reach.

You should also consider the type of cameras you are placing. If you don't have adequate external lighting, then night vision-capable cameras are important. You might want cameras that transmit their signal to a remote location for storage. If you choose to transmit the camera feed, make sure the signal is secure so that someone cannot easily tap into the signal.

12.1.4 Fire Protection

Obviously, a fire will destroy servers and other equipment. Having adequate fire alarms and fire extinguishers in your facility is important. Fire extinguishers can be classified by what types of fire they are able to put out:

- **Class A:** Ordinary combustibles such as wood or paper
- **Class B:** Flammable liquids such as grease, oil, or gasoline
- **Class C:** Electrical equipment
- **Class D:** Flammable metals

Fire suppression systems are common in larger office buildings. These systems are divided into three categories:

- Wet Pipe
- Always contains water
- Most popular and reliable
- 165-degree fuse melts
- Can freeze in winter
- Pipe breaks can cause floods
- Dry Pipe
- No water in pipe
- Preferred for computer installations
- Water held back by clapper
- Air blows out of pipe, water flows
- Pre-action
- Usually recommended for computer rooms
- Basically operates like a dry pipe
- When a certain temperature is reached, water goes into the pipe, then is released when a higher temperature is reached

Having a plan to address fires is important. Depending on budget and security needs, your plan can be as simple as well-placed smoke alarms and a fire extinguisher or as complex as a series of fire suppression systems with an alarm system that automatically notifies the fire department.

Disaster Recovery

12.2 Disaster Recovery

A disaster is any event that significantly disrupts your organisation's operations. A hard drive crash on a critical server is a disaster. Other examples include fire, earthquake, your telecom provider being down, a labour strike that affects shipping to and from your business, and a hacker deleting critical files. Just keep in mind that any event that can significantly disrupt your organisation's operations is a disaster.

12.2.1 Disaster Recovery Plan

You should have a disaster recovery plan (DRP) in place to guide the return of the business to normal operations. This must include a number of items. You must address personnel issues, which means being able to find temporary personnel if needed, and being able to contact the personnel you have employed. It also includes having specific people assigned to specific tasks. If a disaster occurs, who in your organisation is tasked with the following?

- Locating alternative facilities
- Getting equipment to those facilities
- Installing and configuring software
- Setting up the network at the new facility
- Contacting staff, vendors, and customers

These are just a few issues that a disaster recovery plan must address; your organisation may have more issues that would need to be addressed during a disaster.

12.2.2 Business Continuity Plan

A business continuity plan (BCP) is similar to a disaster recovery plan but with a different focus. The DRP is designed to get the organisation back to full functionality as quickly as possible. A business continuity plan is designed to get minimal business functions back up and running at least at some level so you can conduct some type of business.

An example would be a retail store whose credit card processing system is down. Disaster recovery is concerned with getting the system back up and running at full functionality, essentially like the disaster never happened. Business continuity is concerned with simply offering a temporary solution, such as processing credit cards manually.

To successfully formulate a business continuity plan one must consider which systems are most critical for your business and have an alternative plan in case those systems go down. The alternative plan need not be perfect, just functional.

12.2.3 Determining Impact on Business

Before you can create a realistic DRP or BCP you have to do a business impact analysis (BIA) of what damage to your organisation a given disaster might cause. Consider a web server crash. If your organisation is an e-commerce business, then a web server crash is a very serious disaster.

However, if your business is an accounting firm and the website is just a way for new customers to find you, then a web server crash is less critical. You can still do business and earn revenue while the web server is down. You should make a spreadsheet of various likely or plausible disasters and do a basic business impact analysis for each.

An issue to consider in your BIA includes the maximum tolerable downtime (MTD). How long can a given system be down before the effect is catastrophic and the business is unlikely to recover? Another item to consider is the mean time to repair (MTTR). How long is it likely to take to repair a given system if it is down? You must also consider the mean time between failures (MTBF). In other words, how frequently does this particular service or device fail? These factors help you to determine the business impact of a given disaster.

All of this data will lead you to a recovery time objective (RTO). That is the time by which you intend to have a service back up and running, should there be a failure. This should always be less than the MTD. For example, if the MTD for your e-commerce server is 48

hours, your RTO might be set at 32 hours, providing a significant margin of error.
Another important concept is recovery point objective (RPO). This is how much data you can tolerate losing. Imagine you do a backup every 10 minutes. If the server you are backing up fails seconds before the next backup, you will have lost 9 minutes and about 55 to 59 seconds of work/data. That will all have to be redone manually. Is this tolerable? That depends on your organisation.

12.2.4 Testing Disaster Recovery

Once you have both a DRP and a BCP, you need to periodically test those plans to ensure they will actually work as expected. There are five types of tests, in order from the least intrusive, easiest to conduct, to the most difficult but most informative type of test.

12.2.4.1 Document Review/Checklist

This type of testing is usually done by an individual. The BCP and/or DRP are simply reviewed to see if everything is covered. They are compared to check lists, perhaps check lists from various standards (like PCI).

12.2.4.2 Walkthrough/Tabletop

This is a team effort. A team sits in a conference room and goes through the BCP and/or DRP and discusses scenarios. For example, "What if there was a fire in the server room?" Then the plans are consulted to see if that is covered adequately and appropriately.

12.2.4.3 Simulation

The purpose of this type of test is to simulate some sort of disaster. A team or an individual might conduct this type of test. It involves moving around in the organisation and asking specific individuals "what if" scenarios. For example, you might ask the database administrator "What is the plan should our financial data server crash now?" The purpose of this is to see if everyone knows what to do if a disaster occurs.

12.2.4.4 Parallel

This test is about seeing if all backup systems come online. That would include restoring backup media, turning on backup power systems, initializing secondary communication systems, etc.

12.2.4.5 Cut-off/Full Interruption

This is the ultimate test. You actually shut down real systems and see if the BCP/DRP works. From one perspective, if you do not ever do this level of testing, then you do not really know if your plans will work. However, if this goes wrong, then you have just caused a disaster. To avoid generating a disaster, there are some steps you can take. The first is to not even consider this test until you have successfully completed the previous tests. In fact, all of these tests should be done in order. First, do a document/check list. If and only if that is successful, then move to a tabletop. Then if that works move to a simulation.
Secondly, you should schedule this type of test during downtime for the company. At a time when, if things go wrong, it will cause the least impact on the business. For example, if this is a bank, then do not do this test Monday morning. Perhaps Saturday afternoon would be best. This would give you a chance to fix anything that goes wrong.

Fault Tolerance

12.3 Fault Tolerance

At some point, all equipment fails, so being fault tolerant is important. At the most basic level fault tolerance for a server means having a backup. If the server fails, did you back up the data so you can restore it? Although database administrators might use a number of different types of data backups, from a security point of view the three-primary backup types are:

- **Full:** All changes
- **Differential:** All changes since last full backup
- **Incremental:** All changes since last backup of any type

Consider a scenario where you do a full back up at 2 a.m. each morning. However, you are concerned about the possibility of a server crash before the next full backup. Therefore, you want to do a backup every two hours. The type of backup you choose will determine the efficiency of doing those frequent backups and the time needed to restore. Let us consider each type of backup in a crash scenario and what would happen if the system crashes at 10:05 a.m.

- **Full:** In this scenario you do a full back up at 4 a.m., 6 a.m., …10 a.m., and then the system crashes. You just have to restore the last full backup, which was done at 10 a.m. This makes restoration much simpler. However, running a full back up every 2 hours is very time consuming and resource intensive and will have a significant negative impact on your server's performance.
- **Differential:** In this scenario you do a differential backup at 4 a.m., 6 a.m., …10 a.m., and then the system crashes. You need to restore the last full backup done at 2 a.m., and the most recent differential backup done at 10 a.m. This is just a little more complicated than the full backup strategy. However, those differential backups are going to get larger each time you do them, and thus more time consuming and resource intensive. Although they will not have the same impact as doing full backups, they will still slow down your network.
- **Incremental:** In this scenario you do an incremental backup at 4 a.m., 6 a.m., …10 a.m., and then the system crashes. You need to restore the last full backup done at 2 a.m., and then each incremental backup done since then, and they must be restored in order. This is a much more complex restore, but each incremental backup is small and does not take much time nor consume many resources.

There is no "best" backup strategy. Which one you select will depend on your organisation's needs. Whatever backup strategy you choose, you must periodically test it. The only effective way to test your backup strategy is to actually restore the backup data to a test machine.

The other fundamental aspect of fault tolerance is RAID, or redundant array of independent disks. RAID allows your servers to have more than one hard drive, so that if the main hard drive fails, the system keeps functioning. The primary RAID levels are described here:

- **RAID 0** (striped disks) distributes data across multiple disks in a way that gives improved speed at any given instant. This offers NO fault tolerance.
- **RAID 1** mirrors the contents of the disks, making a form of 1:1 ratio real-time backup. This is also called mirroring.
- **RAID 3 or 4** (striped disks with dedicated parity) combines three or more disks in a way that protects data against loss of any one disk. Fault tolerance is achieved by adding an extra disk to the array and dedicating it to storing parity information. The storage capacity of the array is reduced by one disk.

- **RAID 5** (striped disks with distributed parity) combines three or more disks in a way that protects data against the loss of any one disk. It is similar to RAID 3 but the parity is not stored on one dedicated drive; instead parity information is interspersed across the drive array. The storage capacity of the array is a function of the number of drives minus the space needed to store parity.
- **RAID 6** (striped disks with dual parity) combines four or more disks in a way that protects data against loss of any two disks.
- **RAID 1+0** (or 10) is a mirrored data set (RAID 1) that is then striped (RAID 0), hence the "1+0" name. A RAID 1+0 array requires a minimum of four drives: two mirrored drives to hold half of the striped data, plus another two mirrored for the other half of the data.

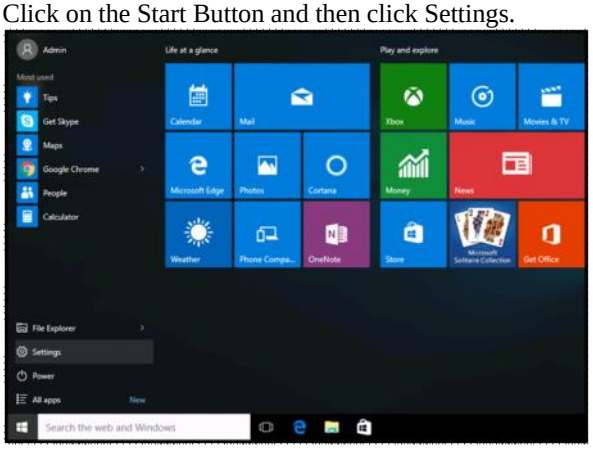
Guided Exercise: Backup Windows 10

12.4 Guided Exercise: Backup Windows 10

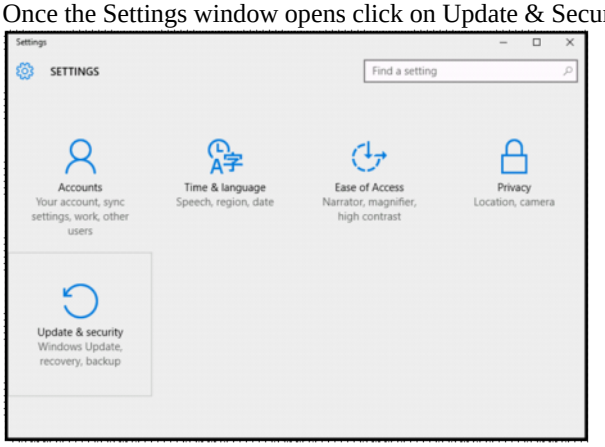
Resources	
Files	None
Machines	Windows 10

In this exercise you will create a full backup of the Windows 10 machine.

Click on the Start Button and then click Settings.

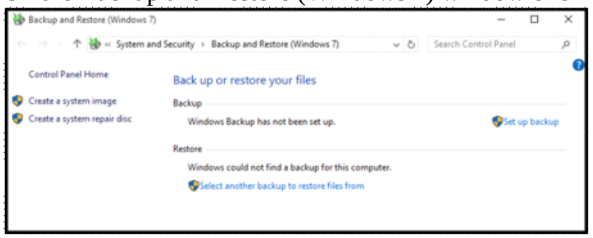


Once the Settings window opens click on Update & Security button.

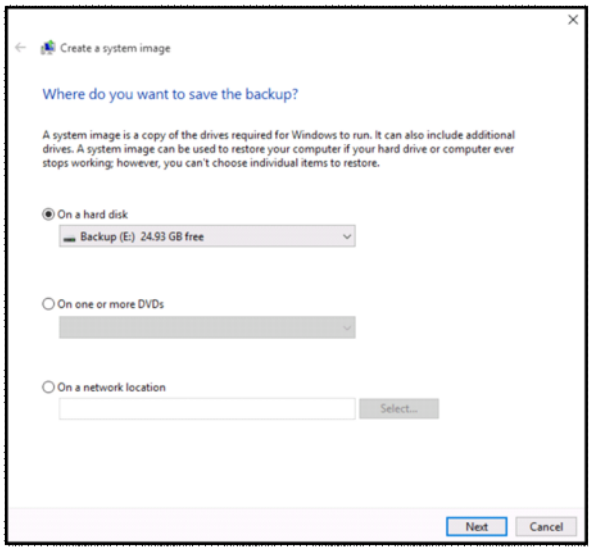


Then select Backup from the menu on the left and click on "Go to Backup and Restore (Windows 7)"

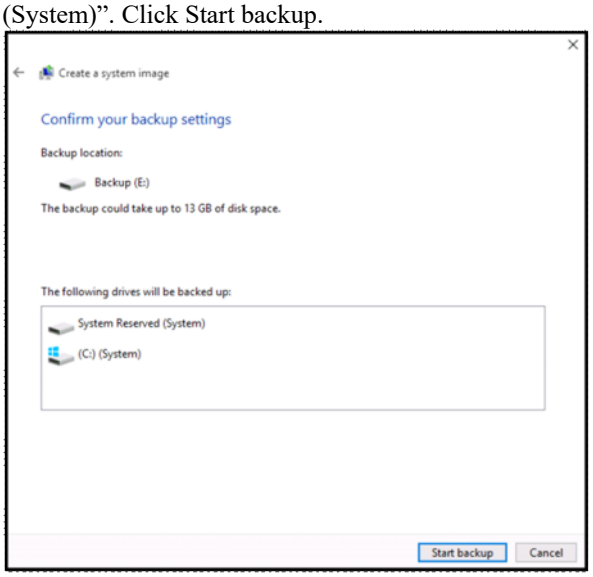
On the Backup and Restore (Windows 7) window click on Create a system image.



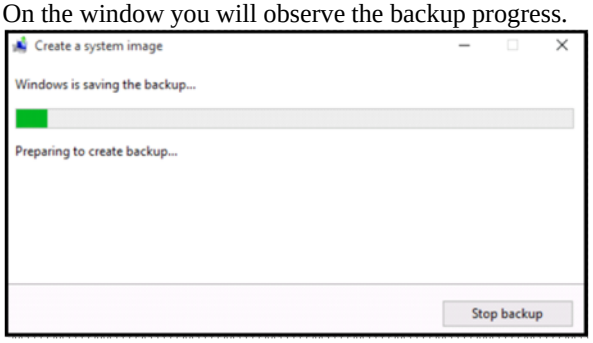
On the Create a system image window select the first option "On a hard disk" and ensure the Backup (E:) drive is selected. Th en click Next.



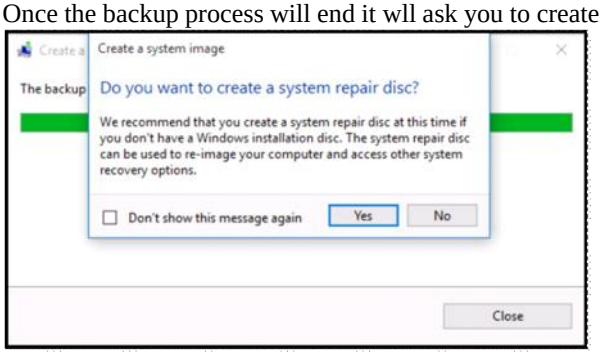
On the next window you can observer which drives will be backed up. In this case it should be “System Reserved (System)” and “(C) (System)”. Click Start backup.



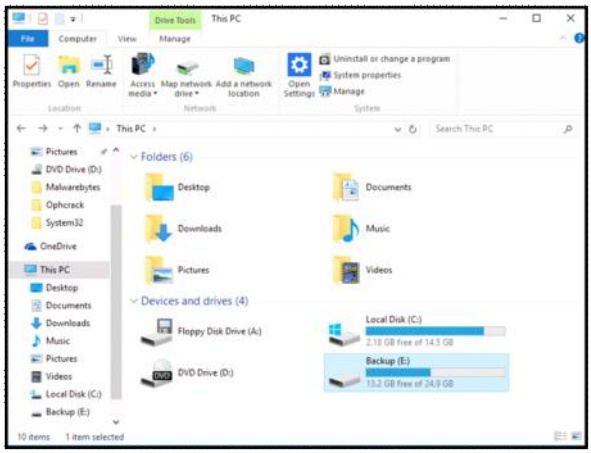
On the window you will observe the backup progress.



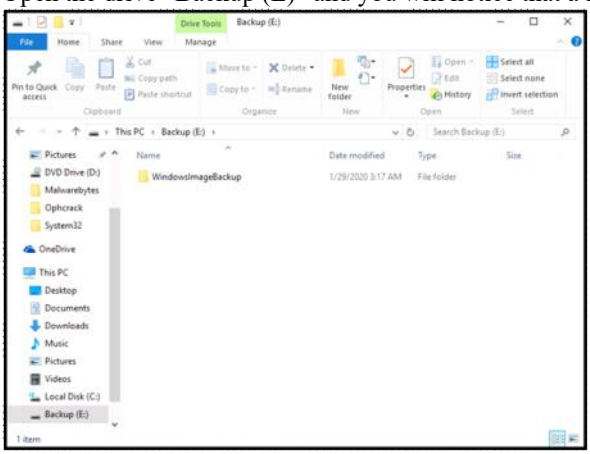
Once the backup process will end it wll ask you to create a system repair disk. At this time click No, and then Close.



Open File Explorer and he click on “This PC”. You will observe that the drive “Backup (E)” has 13 Gb free from 25GB.



Open the drive “Backup (E)” and you will notice that a folder exists called “WindowsImageBackup” which contains the backup files.



QUIZ:

- 1.The disaster recovery plan has as a major goal to get the organisation back to full functionality.
- 2.Which of the following is NOT considered a disaster?
- 3.How should a company test the integrity of its backup data
- 4.Which RAID level uses mirroring?
- 5.What is a mantrap?
- 6.The plan for recovering from an IT disaster and having the IT infrastructure back in operation is called?
- 7.RAID 0 does not offer fault tolerance
- 8.A common method of securing building access is to have a locked door or barrier requiring employee ID.
- 9.Which RAID level offers dual parity
- 10.Cameras must be placed so that they have an unobstructed view of the areas you want to monitor.