==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4001.mp4 ====
understanding the basics and tools is only part of the battle a robust security plan involves the strategy of searching for vulnerabilities addressing them before any attackers do and planning for any interruptions to critical business functions in this domain we will cover identifying vulnerabilities managing risk and developing disaster recovery and business continuity plans vulnerability management is an ongoing process in which organisations proactively identify vulnerabilities document discovered vulnerabilities make decisions on how to handle those vulnerabilities and what order implement responses to mitigate the most important vulnerabilities and monitor how effective deploy responses are managing vulnerabilities is always more effective and less costly than dealing with the consequences of successful attacks the first step in vulnerability management is to identify vulnerabilities that exist in an environment the first step in vulnerability identification is to collect comprehensive descriptive information about an environments hardware and software components a comprehensive inventory is made up of descriptive information for each component including detailed version information once a comprehensive inventory has been compiled each component can be compared against lists and databases of known vulnerabilities to identify intersections that indicate a vulnerability exists for one or more deploy components food fresh knows that good cybersecurity builds customer Trust so their it organisation implemented a change control process that documents all configuration changes to their it infrastructure they are confident that their software and hardware Inventories stay up to date but they still scanned verify periodically and stay current on the latest vulnerabilities the fact that a vulnerability exists for a diploid component does not necessarily mean that an attack is imminent for a vulnerability to be exploited there must be an external threat that is realised against that specific vulnerability the main purpose of vulnerability management is to reduce and organisations attack surface by mitigating as many vulnerabilities as possible within budgetary constraints as a result of organisations operating with limited budgets the best approach to implementing vulnerability mitigations is to qualitatively and or quantitatively assess the relative impact of each discovered vulnerability and apply budget to vulnerabilities deemed most damaging once the organisation decides which vulnerabilities will be mitigated the goal is to reduce the opportunity for an attacker to successfully exploit a vulnerability and carry out an attack mitigating a vulnerability does not always mean removing that vulnerability it means to make it less dangerous to the organization the last step in

vulnerability management is to assess each mitigation to ensure that the exposure to each vulnerability is less than it was before deploying mitigations if you're mitigations are doing their job your organization's attack service should be smaller at this point the process repeats itself and continually results in finding new vulnerabilities and ways to mitigate them

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4002.mp4 ====
attackers and cybersecurity professionals both use reconnaissance to gather information about a target environment attackers use reconnaissance to identify the weakest component or components in an environment in cybersecurity professionals carry out the same tasks to identify vulnerabilities before the attackers do there are two main types of reconnaissance that are helpful to build a picture of a target environment passive reconnaissance is the process of collecting information about a target environment without interacting with that environment directly active reconnaissance collects environmental information by interacting with the environment and analysing responses knowing how to use active and passive reconnaissance prepares an organisation to build a solid defense from cyber-attack in advantage of passive reconnaissance is that information collection can occur in stealthy manner the target environment is not alerted to passive reconnaissance activities internet search engines and social media can be great sources of information about any organisation or person it doesn't take long to collect demographic and other descriptive information about a target the technique of using an internet search engine to find detailed information about any entity is a process called Google hacking Google hacking involves using specific syntax and constructing Google or other search engine queries to return information about online entities social media accounts for an organisation or its personnel can also return valuable information job postings can also be repositories of valuable environmental information for example if an organisation is advertising for an Apache web server security specialist it stands to reason that that organisation uses the Apache web server job applicant requirements often divulge important environmental architectural details other online resources for passive reconnaissance include sites that published leaked passwords and strategic search engines such as showdown or census open a web browser and navigate to https colon slash slash www.shonenjump.com

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4003.mp4 ====
another useful website for passive reconnaissance is the way back machine which can be found at archive.org the way that machine stores archived versions of websites some of which go back over 20 years you will not find every website represented in this database but for those that do exist looking at old versions of an organization's website can reveal lots of information about that organisation open a web browser and navigate to https colon slash slash archive.org type loki.com the results page shows how many times the website learnt key.com has been captured you can select any date on the calendar to see what the website look like on that day you can see this website has been captured 826 times between November 9th 1996 through March 18th 2022 let's select the year 2007 and pick any date on that calendar look like in 2007 the way that machine can provide lots of information about how companies have changed over time the other main approach to reconnaissance is active reconnaissance when carrying out active reconnaissance the goal is to communicate with the target environment to determine what resources exist within a network and what those Resources do one of the most common tools used for active reconnaissance is in map the in map utility stands for network mapper and fulfills its name quite well within map you can scan a network to find what nodes are active what ports are open on each node and even make an educated guess as to what operating system each node is running an initial in map scan is one that likely just Returns active nodes and helps develop the high level view of a network architecture the process of active reconnaissance used to map a network is called enumeration at the windows powershell prompt type in map minus capital a 10.0 / 24 and select the inner key on your keyboard the in map utility will scan the 10.0.0 network and report on open ports possible operating systems and any other service information it can find there are many other tools available to help collect information from a network including tools like who is netcat in Wireshark each one of these tools assists in collecting information about a network environment by sending network traffic to Nodes in the network and analysing the results active reconnaissance is generally more accurate than passive reconnaissance but at the risk of the person carrying out the reconnaissance being discovered most active reconnaissance utilities generate traffic that network security devices can detect and potentially classify as malicious activity in short if stealth is important use passive reconnaissance first and then only use active techniques sparingly

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4004.mp4 ====
the testing phase of vulnerability identification is really an extension of the active reconnaissance phase testing or port scanning often uses many of the same tools as those used in initial active reconnaissance the main difference is in the intensity of the scan and the quantity of traffic sent to each node a simple icmp packet sent to a suspected node may be sufficient to report that the note is alive but to determine what ports are open and what services are running on each port many more packets will be sent to the same node testing through port scanning is an effective way to collect the same information about your environment that attackers may try to use against you the inmate utility is a favourite tool to use in Port scanning multiple tools are available that either work in a similar fashion to in map or that provide a more user friendly front end map for more sophisticated and unattended port scanning more comprehensive packages such as nessus or openvas provide aggressive port scanning and Environment analysis with user-friendly front ends the main goal of the testing or port scanning phase is to collect as much information as possible about the operating systems and services the target environments nodes are running when an attacker or cybersecurity professional knows what services are running on what nodes identifying which of those components are most vulnerable becomes possible for example if a brand new vulnerability for the Microsoft internet information services or II's web server is published and attacker would want to know if that vulnerability might be an attack vector for specific target if the testing phase reports that a target runs the Linux operating system in the Apache web server no iis vulnerability would do the attacker any good that's why learning as much as possible about each target node helps choose the vulnerabilities that may be the way to compromise one of those nodes

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4005.mp4 ====
in Linux open the greenbone security manager which is the web interface for openvas to do that launch a web browser and navigate to 10.091 type webinar in the username fill in an admin in the password fill in then select sign in select scans to display the task page the wizards icon in the upper left portion of the page and select task wizard to open the task wizard dialog you can initiate a comprehensive scan on a single target or network by typing the IP address in the IP address or hostname fill in and selecting start scan for now select cancel select a wizard icon again and this time select advanced Task wizard to

open the advanced Task wizard dialog in this dialogue you can initiate a scan but you have more control of the scan parameters one of the more flexible parameters you can change here is the type of scan to perform select the scan config drop down arrow and select Discovery type 10.0.0 / 24 and the target host fill in then select create to initiate a Discovery scan for the 10.0.0 / 24 network and then carry out this scan to find out what nodes are running on the network the nature of Port scanning is that it is an iterative process that means that the common approach is to start with high level scans and then create more detailed scans based on the information received in the previous scan layer for example a first-level scan might include an operating system fingerprint pass which means in attempt to determine the operating system for each node taking the results of the phase one scan the next scan could search for common ports that might be open based on the detected operating system this approach requires many more scans and lots of repetitive activity to increase consistency and reduce errors automation can help simplify multiple layers of scans automation can be as simple as writing scripts that call command line utilities or utilising more comprehensive scanners such as nessus or open bass in automating their activities regardless of the nature of the tools it is recommended to automate scans as much as possible to reduce the workload in finding vulnerabilities

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4006.mp4 ====
an important part of vulnerability management is determining what vulnerabilities exist in the scope of an IT environment the standard approach to discovering vulnerabilities is to compare current hardware and software inventory with the repository of known vulnerabilities knowing how to use vulnerability repositories and how to avoid their limitations helps avoid missing important vulnerabilities there are multiple sources of vulnerability repositories available both as lists and databases some repositories are publicly available in others are available by subscription only regardless of the repositories you may choose to use it is important that your inventory Express hardware and software components in a way that you can query the repository for matching vulnerabilities likewise you should use a standard vocabulary for describing vulnerabilities their severity and possible mitigations open web browser and navigate to https colon slash slash cve.mitre.org cde stands for common vulnerabilities and exposures and it is a list of publicly disclosed security flaws maintained by The Mitre organisation this is one of the most common repositories of vulnerabilities that's published to the world select search cve

list and type Apache in the search box and select submit the results show a list of all of the known and published vulnerabilities with the Apache web server or at least that include the word Apache notice there are 2032 records that match your search you scroll through you can see there's lots and lots of vulnerabilities that have been posted here let's select one and you can see a description of a specific cve ID entry with a description of what the vulnerability is the date the record is created and lots of information about the vulnerability and what to do about it vulnerability repositories can dramatically reduce the time required to identify vulnerabilities but they're only useful if the contents of the repository are current since new vulnerabilities are discovered daily and out of date vulnerability repository may miss crucial vulnerabilities that could allow an attacker to compromise your environment that's why it's important to continually scan your networks for running services and compare that result with online up-to-date vulnerability repositories to make sure you're aware of every vulnerability that could impact your environment

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4007.mp4 ====
publicly available vulnerability repositories ease the burden of identifying vulnerabilities using industry standard tools to carry out vulnerability identification reduces the amount of time required and increases the quality of the vulnerability identification process finding more vulnerabilities along with severity information assists assessors in determining which vulnerabilities warrant the strongest response while there is still substantial work to be done using standard tools increases the effectiveness of making recommendations and crafting policies that are aligned with industry-wide best practices many tools including nests openvas and even the Legacy Microsoft baseline security Analyser or mbsa correlate their findings with online publicly available vulnerability repositories and produce standard output and reports that are easy to understand and use in decision-making security manager web interface for openvas to do that launch a web browser and navigate to 10.091 type web admin in the username fill in and admin in the password fill in select sign in select scans then tasks to go to the task page scroll down and you can see there are three scans to a complete and one and still in process the first scan was a scan of the IP address 10.0.0 131 that's actually this current virtual machine the severity shows very little concern and indicates that this node appears to be relatively secure already the next scan however is a different story the IP address 10.045 is another virtual machine that's running an older version of Ubuntu and is configured to be deliberately insecure you can see

the openvas agrees with that assessment a severity of 10.0 means that this node needs more attention select this second report to see the details let's select results to see a list of findings sorted by severity you generally should mitigate the most severe vulnerabilities first let's select CBE to see how each vulnerability maps to an entry in the cve list you can select any link in this list to see more details from CBE let's select the first entry for the first CBE entry so when you first looked at the cve list it's overwhelming although you can go to the cve website and search for your own vulnerabilities it's a lot easier to let a scanning tool find vulnerabilities and then correlate those to existing cve entries here we can scroll down and get an overview of the vulnerability that has been detected and lots of Supporting information on how to confirm it validate it and determining what to do about it this is one of the strongest reasons to use a tool like openvas or nessus or another integrated scanning platform it gives you all the information in one place to determine how to respond to a vulnerability this quick look at openvas is only a brief overview of the product there are many more robust features that help cybersecurity professionals keep their environments more secure

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4008.mp4 ====
want the greatest advantages of a hyper-connected world is that it's very easy to dig up information on any subject there are many online resources that provide threat intelligent information learning from and drawing on current threat intelligence is a prerequisite for an effective vulnerability management program one of the most commonly referenced repositories for vulnerabilities is the one we've already seen the common vulnerabilities and exposures or cve list CBE is maintained by The Mitre corporation and should be the first go to when examining or researching vulnerabilities but cve is not the only source for vulnerabilities and threats a comprehensive threat intelligence program should include staying up to date with cybersecurity reports news items that relate to cybersecurity both free and subscription-based services and participating in collective intelligence exchanges let's go online look at a couple of the resources that are available to help stay current with ongoing threats open a web browser and navigate to https colon slash slash cve website from the CBE website we can search the CBE list by entering keywords that correspond to services or software we have installed we've already done that we can also go to data feeds provide multiple sources of information that you can subscribe to or just consume through a website such as this to keep up-to-date on security information take some time to look

through these various sources of security information find one that speaks to your organisation and use it to stay up to date another great resource to find various threat intelligent feeds can be found at https colon slash slash D3 security.com intelligence dash feeds and once you type all that in you'll find a great resource for threat intelligent feeds spend some time scrolling through the resources on this website and you'll find a source of information that speaks to nearly every industry category and almost definitely you'll find several sources to keep you up to speed on what's going on with respect to threat intelligence some of the more important ones of course include department of homeland security the FBI in for guard portal is one that many cybersecurity professionals use there's ransomware tracker the Sands internet storm Center is another resource I would recommend that you take a look at and of course there's many more the idea is to develop an ongoing process of staying up to date on what's going on in the cybersecurity world

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4009.mp4 ====
threat intelligence awareness operates at least two levels it is important to stay abreast of the current state of cybersecurity and ongoing threats but sometimes it is necessary to dig little deeper when suspected activity is discovered ad hoc threat intelligence describes the process of researching suspicious activity to determine if that activity is the result of a potential attack or preparation for an attack ongoing thread intelligent preparedness is the process of frequently visiting sites and Resources that contain updates news and summaries of ongoing cybersecurity topics automating thread intelligence activities is an absolute necessity to keep up with a fast-changing security landscape automation can include scripting frequent vulnerability scans utilising vulnerability assessment suites in their automation features and integrating schedule scans with updated vulnerability database and security feeds many information feeds provide apis that allow sophisticated scripts to automatically investigate vulnerability results to help stay current with emerging threats let's take a look at a few online threat intelligence resources the first is naked security at https colon slash slash make it security.com make it security publishers a podcast and pertinent articles that cover current cybersecurity topics their articles are sorted by date that you could search by keyword to find just what you're looking for the next resource is the sans internet storm center at https colon slash slash iscu the Sands internet storm Center is one of the core resources every cybersecurity professional should frequent this page gives you access to podcasts and diary entries of security

related resources and articles searching the diaries can provide a wealth of information on just about any security topic is threat post thread post is at https colon slash slash threatpost is yet another resource that offers podcasts and articles on current security topics many of the tools and Resources you have already seen support automating the collection and analysis of updated threat intelligence explore these resources to find out how automation can help reduce the daily workload of keeping current

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4010.mp4 ====
the first step in crafting a penetration test cybersecurity attack or carrying out a comprehensive vulnerability assessment is that enumeration phase enumeration is developing the architectural detail plan of your target environment the reason that enumeration is so important in the vulnerability management process is because the whole purpose is to find what vulnerabilities are known that affect the hardware and software components of your network if your hardware and software asset list is incorrect or out of date you're going to miss potentially harmful vulnerabilities in your it environment a critical component of a comprehensive vulnerability management program is ensuring that all documentation pertaining to your it environment is accurate and up-to-date asset lists network Maps policies procedures in any other documentation should be periodically reviewed and updated to reflect the current state of your environment likewise documentation should be reviewed whenever a security incident occurs and after the incident has been resolved since the security incident can only occur when an attacker exploits a gap it is important to address any gaps in document any changes that were made assume that food fresh added a new web server to their environment to handle new line of allergen free food products if administrators neglect to add the new web server to the hardware and software asset list subsequent vulnerability assessments will ignore the new web server and potentially miss any vulnerabilities that are present while omitting a specific server or service does not always lead to an attack it does open the door for potential vulnerabilities to be found by an attacker if the system owner is not looking at the resource themselves that is why a change management process is so important to security keeping documentation up to date may not be easy but it will make your it environment much more secure and more shorten the time required to respond to incidents

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4011.mp4 ====
you may have heard the term risk management and vulnerability management used interchangeably in reality vulnerability management and risk management are related but they are distinct activities understanding the difference between a vulnerability and risk help security professionals develop the most effective strategies to avoid cyber attack a vulnerability is any Weakness in an environment that could allow an attacker to carry out a successful attack to carry out a successful attack and attack her must carry out and exploit against a vulnerability a risk is the likelihood that some action may occur that has an effect on an organisation along with the magnitude of the impact to that organisation in most cases and in our conversation of cybersecurity We Will consider risk to refer to an adverse event regardless of the approach used to assess risk the primary goal is to create a list of known risks sorted by likelihood and effect on the organisation any action that exploits a vulnerability successfully is referred to as a realised risk realise risk always has an effect on the organisation and the ones that are most likely to occur and had the highest negative impact are the ones that should be addressed first one approach to mitigating risk is to mitigate the vulnerability which could allow risk to be realised that's why vulnerability management and risk management are related processes

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4012.mp4 ====
there are two main approaches to assessing and managing risk qualitative and quantitative it is important for security professionals to understand both qualitative and quantitative risk assessment methods and know when to use each one to build an effective risk response plan qualitative risk assessment assigns a subjective level of risk based on an individual risks likelihood of occurrence and effect on the organisation each organisation can define its own levels of risk the common risk levels include low medium high and extremely high a risk that is likely to occur several times each year and will result in a loss of several hundreds of thousands of Dollars with each occurrence would likely be assigned a risk of high or extremely high on the other hand a risk that is expected to only be realised once every 10 or 15 years with an expected loss of $500 per occurrence would be assigned a risk level of low qualitative risk assessment is good for comparing the relative importance of different risks but not comparing monetary impact quantitative risk assessment assigns numbers that are easy to calculate and use in

formulas to determine expected loss each risk is a sign of probability of occurrence and a Dollar value for the loss should that risk be realised the Dollar value of the realised risk loss is easy to calculate by multiplying the occurrence probability times the loss expectancy quantitative risk analysis makes it easy to write risk by expected loss each year quantitative risk assessment works very well when numbers are available and can be largely automated however occurrence probabilities and expected loss numbers are only estimates it is often the case that personnel who worked most closely with the resources at risk may provide more valuable input to the risk assessment process for this reason it's recommended to use both qualitative and quantitative risk assessment and compare the results the best result of each analysis type would be a list with the same risks ranked in the same manner in practice the lists are likely to be slightly different and require management to make decisions on how to allocate limited budgets for risk mitigation

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4013.mp4 ====
breach identified risk their generally four mitigation options organisations can choose any of the four depending on its applicability to a specific risk one way to mitigate risk is avoidance any risk that can completely be avoided without excessive costs should be avoided an example of avoidance can be disabling or removing unneeded services for example if a database server has an old insecure web server running on that same computer the unused web service may be vulnerable to attack disabling the web service or completely uninstalling the web service removes the vulnerability and any risk associated with it another risk mitigation strategy is acceptance if the risk is realised and causes very little negative impact to the organisation the best strategy may be simply to accept the risk if trying to mitigate the risk using some other technique would cost more than the loss that is expected then acceptance may be the best choice any risk that cannot be accepted or avoided may best be handled by being controlled controlling a risk means to deploy some security control that reduces the probability that a risk will be exploited by a successfully realised threat adding a firewall IDS or IP's or implementing nfa or examples of deploying security controls as mitigation strategies and finally the last risk mitigation strategy is to transfer the risk transferring a risk is the result of an agreement that should a risk be realised the loss would be covered by another party insurance is one of the most common risk transference approaches think of your personal vehicle personal car insurance

is an agreement between an account holder and an insurance provider in exchange for a periodic premium pay to the insurance provider the insurance provider agrees to pay for loss due to various types of Damages a key aspect of risk management is to understand the risks that posed the most danger to an organisation and which mitigation strategy provides the most economical protection against each risk

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4014.mp4 ====
possum risks or global across any organisation other risks target specific data data disclosure is a risk for data that should not be disclosed not all data that information systems store or process should be protected from disclosure only data that is marked as sensitive should be protected and controlled from disclosure understanding how data classification affects security control needs is important to building effective security common classes are protected data include personally identifiable information or pii and personal health information or Phi pii and Phi are common targets of standards and regulations to ensure these types of data are protected pci-dss gdpr and hipa are all standards and regulations that set requirements on how pii and Phi are handled special classifications of certain types of data come with additional risk for example disclosing consumer private information or pii for organisations that are subject to gdpr may result in the risk of fine or loss of privileges gdpr does not place the same level of restrictions on non-personal data so in this way data classification should play into overall risk management in short some types of data carry more risk than other types of data

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4015.mp4 ====
comprehensive security assessments of it systems should span all hardware and software components within an IT infrastructure each device is role should inform the level of assessment to ensure the utmost security of that component to yield the most effective security plan servers that have sensitive information should require higher levels of security than other devices that may not be targets to attack however devices that may provide incremental access to higher value servers must be assessed in the overall process as well remember that security is not a state but rather a process an organisation may take a security snapshot at a point in time but any changes to the

environment will likely change the overall security posture a rigorous change management process must be in place and followed to ensure the organisation can keep track of how the infrastructures state changes over time operations on a day-to-day basis both change the state of an infrastructure and gather valuable information on its operation collecting input from operations should be part of the security assessment process end users and help desk personnel can often provide valuable input as to how well or poorly and infrastructure is operating to ensure that all parts of an organisation are working together for more secure environment information Assurance should continually review input provided from all sources to ensure compliance with policy when all the pieces work together environments are more cohesive usable and secure

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4016.mp4 ====
a disaster is any event that results in major disruption to operations disasters come in all forms and understanding the various types of disasters that may occur helps an organisation plan to whether those storms in most cases disasters can be classified as natural or human caused natural disasters include things like earthquakes tornadoes floods and other whether an environmental related events natural disasters can result in short-term disruptions or long-term disruptions a power outage as a result of an Electrical Storm is quite different than a complete loss of a data center due to flood organisations must have plans in place to respond to all types of disasters the other main classification of disaster is a human cause disaster disaster is in this class includes cyber attacks strikes Sabotage terrorism war or even negligence any human action that results in a major disruption to operations can be considered a human cause disaster regardless of the origin of any disaster the main goal is to protect personnel first then restore operations as quickly and efficiently as possible depending on the severity of the disaster recovery may require changes in location infrastructure repair or replacement and various levels of rebuilding any information systems environments

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4017.mp4 ====
organisations should have at least two plans in place to respond to interruptions to operations the Two primary plans needed to survive in eruptions are a disaster recovery plan or drp and a business continuity plan or

BCP organisations who have proper plans in place have a much better chance of surviving an interruption rather than succumbing to it the difference between a drp and a BCP has to do with severity in short a BCP addresses short-term interruptions while a drp addresses severe damage to the infrastructure that supports operations both drp and BCP focus on restoring minimal business operations before an organisation can plan to continue or restore operations they must have a clear understanding of what makes up their operations a business impact analysis or BIA is a formal assessment of business processes that are Critical to support normal operations a comprehensive via defines all critical business functions or CBS that must be protected to conduct operations the drp and BCP provide details on what it takes to ensure that all CVs can operate a BCP is a plan that is activated whenever one or more CBFS are interrupted and interruption can be as simple as a power outage or a malfunctioning hvac system which causes workers to leave a facility a BCP often specifies alternate processing options that allow CBS to continue with minimal interruption bcps often depend on redundancy and alternate approaches to maintaining CBF continuity a drp gets activated whenever an event has caused so much damage that the infrastructure that supports operations can no longer function fires earthquakes and other major events that cause structural damage are often causes to activate a drp the drp specifies the steps necessary to take to restore the infrastructure that operations needs to continue once the drp satisfies its goals the BCP can continue to restart operations the two plans work together when necessary to ensure that an organisation experiences the minimum downtime possible during an interruption or disaster

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4018.mp4 ====
a backup is one of the most common components of a BCP and drp that allows operations to continue organisations that do not create backups risk losing critical operational data that may result in substantial monetary losses a backup is simply a secondary copy of stored data to be used if the primary copy becomes damaged or otherwise unusable historically most organisations would create periodic backups to removable tape devices today backups may use tapes but may also utilise removable disks optical disks network storage or even virtualised images the primary goal of the backup is to copy important data to an alternate source with the hopes of separating the backup from the source of any damage that may occur to the primary copy since backups should be separated from primary copies removable Media or network storage

is often desirable geographically separated backups decrease the possibility that a catastrophic event will impact both the primary and secondary copies of data for that reason off-site backups and alternate processing sites are common to help organisations be resilient in the face of localised disasters let's take a look at creating a backup using Windows Server in Windows Server select start and type backup select Windows Server backup from the actions pane on the right-hand side of the screen select backup schedule helps you build a backup schedule through multiple steps where you first select the backup configuration if we select next we see we have full server or I could customise select next I get to select the backup time once a day or more than once a day and if it's more than once a day I can select what times I want select next we then get to determine where we want to store the backups once we determine where we tell Windows what disc we want to back up to and finally we confirm the process this is how easy it is to set up a new backup schedule you want to make sure you back up periodically add a set schedule so that you always know you have a good secondary copy of data available one of the most common flaws in a backup strategy is a clear procedure for restoring backup data when needed restoring a backup image is not always as easy as organisations may expect the process involves acquiring the correct backup image determine what parts need to be restored and then initiating the restore process all the steps depend on proper backup handling labeling and scoping of the restore process without proper planning and organisation may find themselves in a situation where restoring a complete backup takes many more hours than expected to avoid surprises after a catastrophic incident organisations must develop comprehensive restore plans and then test them any untested recovery plan is in and of itself a disaster waiting to happen

==== C:/Users/Kassem Anis/OneDrive - Debreceni Egyetem/Asztal/HPOTest/videos/D4019.mp4 ====
what are the primary tenets of cybersecurity is availability a disaster that interrupts operations is in effect and attack on availability implementing controls to reduce the risk of a disaster impacting operations is a crucial aspect to maintaining availability although the focus of cybersecurity controls is to protect against attack a disaster can be viewed as a specific category of attack one of the first layers of disaster controls are preventative controls preventive controls are controls that are designed to prevent and attack or incident from occurring in the case of a fire using fireproof materials when building a data center and prohibiting flammable contents or open flames

within the context of the data center can help prevent a fire further installing appropriate electrical circuits and periodically examining electrical cabling and electrical connections can reduce or prevent fires Started From electrical faults the next layer disaster controls are detective controls fires only one type of disaster in which damage increases dramatically as the event persists early detection of a fire is crucial to control damage and avoid a series incident from becoming a full-fledged disaster fire detection devices such as smoke detectors are a first line of Defense in fighting fires once a fire is detected the next line of Defense is a corrective control fire extinguishers provide the ability to respond or correct a fire that has been detected fire extinguishers exist in different classes to be used for different types of fires comprehensive disaster preparation should include all three types of controls for each identified disaster threat