Google IT Support Specialization

Course 4: System administration and IT infrastructure services

05 Data recovery backups

Table des matières

[1 Introduction to system administration and IT infrastructure services 2](#_Toc14193580)

[2 Network and infrastructure services 2](#_Toc14193581)

[3 Software and platform services 2](#_Toc14193582)

[4 Directory services 2](#_Toc14193583)

[5 Data recovery backups 2](#_Toc14193584)

[5.1 Planning for data recovery 2](#_Toc14193585)

[5.1.1 Module introduction 2](#_Toc14193586)

[5.1.2 What is data recovery 2](#_Toc14193587)

[5.1.3 Backing up your data 3](#_Toc14193588)

[5.1.4 Backup solutions 3](#_Toc14193589)

[5.1.5 Testing backups 4](#_Toc14193590)

[5.1.6 Types of backup 4](#_Toc14193591)

[5.1.7 User backups 5](#_Toc14193592)

[5.2 Disaster recovery plans 6](#_Toc14193593)

[5.2.1 Whats a disaster recovery plan 6](#_Toc14193594)

[5.2.2 Designing a disaster recovery plan 7](#_Toc14193595)

[5.3 Post mortems 8](#_Toc14193596)

[5.3.1 Whats a post mortem 8](#_Toc14193597)

[5.3.2 Writing a post mortem 9](#_Toc14193598)

# Introduction to system administration and IT infrastructure services

# Network and infrastructure services

# Software and platform services

# Directory services

# Data recovery backups

## Planning for data recovery

### Module introduction

Have you ever had something unexpected and catastrophic happen to a piece of tech you owned? Maybe you dropped your cellphone and it shattered or spilled a glass of water all over your laptop. I know it's happened it to me, and no, it's not fun. While hardware may be hard to replace, data can be even harder to get back, especially lost photos of special moments, important documents and more. In this module we're going to arm you with tools you need to be prepared for these accidents, so you can minimize the impact and loss of data. All right, let's get right into it, data recovery.

### What is data recovery

What exactly is data recovery? If you've ever broken a cell phone, you probably lost some good pictures along with the phone itself. Data recovery is a process of attempting to recover the data that's lost from the broken phone. But this is just one example of attempting to recover from unexpected data loss. Data recovery, in general terms, is the process of trying to restore data after an unexpected event that results in data loss or corruption. Maybe a device that contains data was physically damaged, or an attacker performed malicious actions, or malware deleted critical data. Whatever the cause, the effect is the same. You suddenly lost some really important data and you need to figure how to get it back. How you go about trying to restore this lost data depends on a few factors. One, is the nature of the data lost. If a device has been damaged, you might be able to recover data from the damaged hardware. This could involve using data recovery software, which can analyze failed hard disks or flash drives and try to locate and extract data files. Another factor that would effect your data recovery is the presence of backups. If you're lucky, or you had the foresight to plan for the unexpected, you have data backed up. And you can restore the data that was lost. Data recovery is an important part of an IT system or organization. Since data is critical component of any business operations, as an IT support specialist, part of your role is to ensure that this data is available and protected from corruption or loss. So, if something goes wrong, the organization can continue with their business operations with minimal disruptions. That's why it's critical to be able to recover from unexpected events that could impact your business data. When an unexpected event occurs, your main objective is to resume normal operations as soon as possible, while minimizing the disruption to your business functions. By the end of this module, you'll have practical tools and methods that you can use to protect your data. One of the most important techniques you'll learn is how to effectively backup your data. The best way to be prepared for a data-loss event is to have a well-thought out disaster plan and procedure in place. Disaster plans should involve making regular backups of any and all critical data that's necessary for your ongoing business processes. This includes things like customer data, system databases, system configs and financial data. You'll learn more about how to design and implement a data disaster plan throughout this module. And lastly, you'll learn more about what IT folks call a post-mortem. Imagine that something did go wrong with your systems and you had to use a disaster plan. You might have discovered issues when recovering your data, that wasn't covered in the disaster plan. A post-mortem is a way for you to document any problems you discovered along the way, and most importantly, the ways you fixed them so you can make sure they don't happen again. Being unprepared for a major data loss event can and has severely impacted businesses. In the upcoming lessons, you'll learn how to prepare for data loss, which is a key part of any IT role. If you're interested in hearing more about how real companies have been impacted by unexpected data loss, check out the supplementary reading. Otherwise, we're going to kick start our journey of data recovery with learning how to backup data, ready? Let's get started.

### Backing up your data

So, you want to protect your organization from critical data loss. Good instincts. But where do you start? Let's run down some of the key things to keep in mind when designing a data backup and recovery plan. The first thing to figure out is what data you need to backup. In a perfect world, you should only be backing up data that's absolutely necessary for operations and can be found in another source. So, things like e-mails, sales databases, financial spreadsheets, server configurations, and databases, should all be included. But what about the downloads that are in your laptop? Is it really necessary to backup all those cat pictures too? Probably not. Backing up data isn't free. Every additional file you back up takes up little more disc space, increasing the overall costs of your backup solution. Once you've figured out what data you like to back up, you should find out how much total data you currently have. But it's not enough just to think about what your backup storage requirements are right now. Your organization may continue to grow and your backup needs should grow with it. Make sure that you account for future growth and choose a solution as flexible enough to easily accommodate increases in data backups. Data can be backed up either locally to systems on site, or the backup data can be sent upside to remote systems. Both approaches have positives and negatives, and can help reduce different risks. The advantage of onsite backup solutions is that the data is physically very close. This makes accessing the data a lot quicker. You won't need as much outbound bandwidth since you aren't sending the data out of your internal network. If you need to restore data from backups, that should happen pretty quickly since the data is close at hand. But one of the unexpected events is a building fire. Now, the systems we were backing up along with the backup server had been lost in the fire. Yikes. We've lost everything. This is why offsite backups are strongly recommended. This involves making backups of critical data and sending the backup data offsite to remote systems in a different physical location. This could be another backup server that you control in a different office, or a cloud hosted backup service. But there are trade offs. Offsite backups better prepare us for catastrophic events that can wipe out data from an entire office, but sending data offsite means that you need to transmit the data outside of your network. This means you need to consider things like encryption and bandwidth. Your internet connection will be used to transmit the backup data. Depending on how much data you're sending off site and how fast the internet connection is, this could take a lot of time. Another important thing to consider is encryption of backups. Since backups will often contain sensitive and confidential business data, it's important the data is handled securely and stored in a way that prevents unauthorized access. When sending data offsite is especially important to make sure that data is being transmitted securely, preferably encrypted via TNS. But that's not all. The resulting backup data that's stored should also be encrypted at rest. This is just good security practice. In the next video, we will discuss some of the practical tools you can use to backup your data.

### Backup solutions

So you're looking to bring a backup solution into your organization. But how do you chose between a DIY backup system or one of the many cloud providers? Well let's start by looking at the tradeoffs between the two. On site, or self managed backups, could be as simple as buying a commercial NAS device, loading it with a bunch of hard drives, and sending data to it over the network. This would definitely work, but it might not be the best long term solution. How do you grow the disk capacity when you need more storage space? How do you handle the failed hard disk? Because hard disks will fail eventually, by the way, it's important to call out these options aren't mutually exclusive. There's nothing stopping you from implementing both on site and offsite backups. Actually, it's often recommended to have both if it's within your organization's budget. One thing that you should consider when evaluating the backup strategy for an organization is, backup time period. How long do you need to hang on to backups for? This answer will impact your long term storage needs and overall costs to maintain a backup system. One approach, which balances cost with convenience, is to archive older data using a slower but cheaper storage mechanism. The standard medium for archival backup data storage is data tapes. These are a lot like audio cassette tapes since they use spools of magnetic tape run through machines that allow data to be written to and read back from the tape. Tape storage is pretty cheap, but isn't as easy or quick to access as data stored on hard drives or solid state drives. This storage system is usually used for long term archival purposes, where data isn't likely to be needed. If it is needed some delay in getting the data isn't a concern. There are dozens and dozens of backup solutions available, we won't cover specific ones since there are way to many. But we'll cover some common tools and give you some examples of backup solutions available. One is the command line utility rsync. Rsync isn't explicitly a backup tool, but it's very commonly used as one. It's a file transfer utility that's designed to efficiently transfer and synchronize files between locations or computers. Rsync supports compression and you can use SSH to securely transfer data over a network. Using SSH, it can also synchronize files between remote machines making it super useful for simple automated backups. Apple has a first party backup solution available for their, Mac operating systems called it Time Machine. It operates the using an incremental backup model. Time Machine supports restoring an entire system from backup or individual files. It even allows restoring older versions of backup files. Microsoft also offers and first party solution called Backup and Restore. This has two modes of operation, as a file based version where files are backed up to a zip archive. Or there's the system image where the entire disk saved block by block to a file. File based backup support, either complete backups or incremental ones. System image backups support differential mode, only backing up blocks on the disk that have changed since the last backup. If you want to learn more about these tools, follow the links and supplemental readings after this lesson.

### Testing backups

There's one last super important topic when it comes to backups. Testing them. The field of IT is littered with tragic tales of IT support specialist and sysadmins attempting to restore data from a back up after a data loss incident, only to discover that their backups are invalid. That's not just embarrassing, it's completely terrifying. The takeaway here is that it isn't sufficient to just set up regular backups. That's only half of the equation. The other half is a recovery process and that process needs to be tested regularly. Restoration procedures should be documented and accessible so that anyone with the right access can restore operations when needed. You don't want your time off to be interrupted because your colleague back at the office doesn't know how to restore the sequel database from the back up, right? Of course not. So document the procedure and make sure you regularly test the documentation to make sure it works now and in the future. This process is called Disaster Recovery testing and is critical to ensuring a well functioning recovery system. Disaster recovery testing should be a regular exercise that happens once a year or so. It should have different teams including I.T. support specialists going through simulations of disaster events. They'll test and evaluate how well-prepared or unprepared your organization is when lots of unexpected events. These scenarios can be anything from a simulated natural disaster, like an earthquake to a fictional, event like a horde of zombies shutting down an office. If that's the case, back ups would be the least of your worries. But it's still important, whatever the scenario, it will your I.T. teams test their emergency procedures and figure out what works and most importantly what doesn't. These simulated events are the perfect way to discover any gaps in your planning. If you discover that you aren't protected from data loss in any given scenario, it's an opportunity to learn and fix this gap without risking real data loss. Sounds like a win-win, doesn't it?

### Types of backup

So we've talked about how important backups are, and why you should be backing up any important data. And some tools that can be used to help you back up data. But how exactly do you decide when, and how to back up data? Well let's explore those options. There's a couple of ways to perform regular backups on data that's constantly changing. You can do a full backup on a regular basis, which involves making a copy of the data to be fully backed up. The full unmodified contents of all files to be backed up is included in this backup mechanism whether the data was modified or not. In the case of data that doesn't change very often, like operating system configuration files, this approach can be inefficient. You're backing up multiple copies of data that isn't changing, which waste space and uses bandwidth unnecessarily. That doesn't seem like the best idea does it?

A more efficient approach is to only backup files that are changed, or been created since the last full backup, this is called a differential backup. The advantage is that you aren't storing backups of duplicated, unchanging data, only the files that changed are backed up. Saving us some storage space and time to form the backup. But you wouldn't want to completely stop taking full backups. Over time you wind up tracking and storing lots of copies of files that change a lot, which will also take up more and more disk space over time. To avoid this it's a good practice to perform infrequent full backups, while also doing more frequent differential backups. How often you perform a full backup will depend on how far back you want changes to be tracked. Let's say we perform full backups once every week, and differential backups daily. In the worst case scenario we'll lose close to 24 hours of data changes, that's not bad.

Another efficient way to backup changing data is to perform regular incremental backups. While a differential backup backs files that have been changed or created, and incremental backup is when only the data that's changed in files is backed up. This is even more efficient in terms of both disk space, and time required compared to differential backups. Again you'll want to use frequent incremental backups along with less frequent full backups. But because this approach only sorts differences in the files that have changed since the last incremental backup, it's possible that all incremental backups are needed to fully reconstruct the files. If one of these incremental backups is missing or corrupt it might not be possible to recover data any more recently than the last full back up. Another drawback is that recovery might be more time consuming. This is because the most recent version of backed up data has to be recreated by integrating the last full backup with each incremental backup that follows. For super large files that are changing frequently this could require a lot of time to process.

One more thing backup systems can do to help save space is bar compression. When creating a backup all the files and folder structures will be copied and put into an archive. Archives are useful for keeping files organized and preserving full structure. Besides archiving the files, backups can also be compressed, this is a mechanism of storing the same data while requiring less disk space by using complex algorithms. Those are way to complicated to go into detail here, but it's important to call out that not all data types lend themselves to being compressed. This means that space savings from compression will depend on what you're backing up. Another thing you should know about compressing backups is the expense of restoration. To recover data from a backup it needs to be decompressed first. Depending on the size of your backups this could take a lot of time, and disk space to expand. We touched on backup storage location a bit in the last lesson, but let's dive into a little more detail. Good news, there's a pretty cheap and easy to maintain option out there for storing backup data on site. You can use a commercial NAS device, or configure a filer server with a large amount of disk space. Wherever you chose to store your backup data you'll need a lot of space. You could go out and buy a giant 10 terabyte hard disk, which could work for a little while. But what do you do once your back up data grows to fill that one disk? Are they even making disks larger than 10 terabytes yet? Another thing to worry about is what do you do if that one disk holding all your backed up data fails. Yikes, that wouldn't be good. These are issues a RAID array can address. RAID stands for Redundant Array of Independent Disks, it's a method of taking multiple physical disks and combining them into one large virtual disk. There are lots of types of RAID configuration called levels. Depending on the characteristics desired from the RAID, various RAID levels prioritize features like performance, capacity, or reliability. RAID arrays are a great, inexpensive way of creating a lot of data capacity, while minimizing risk of data loss in the event of disk failure. They can even be flexible enough to allow future growth in disk capacity. We won't go into the nitty gritty details of the different RAID levels available, but if you want to learn more check out the supplemental readings at the end of this lesson. I want to stress the fact that RAID isn't a back up solution, it's a data storage solution that has some hardware failure redundancy available in some of the RAID levels. But storing data on a RAID array doesn't protect against accidentally deleting files, or malware corrupting your data. This is so important that I'm going to say it one more time. RAID is not a replacement for backups.

### User backups

As an IT support specialist working closely with users in your organization, the topic of users backups is sure to come up. We've already covered backing up mission critical operational data, but what about the spreadsheets and PDX and Karlie's laptop. She's going to want to make sure that she doesn't lose those if her laptop gets stolen. While it's important to have a backup solution for infrastructure and critical systems, you also to think about your users and their valuable files. Ensuring reliable backups for client devices is a bit more challenging than infrastructure devices. There likely to be lots of more client devices to backup compared to infrastructure ones. Plus there are laptops, phones and tablets that won't be in the office all the time. One solution to user backups is to use a cloud service designed for syncing and backing up files across platforms and devices. Some examples of these are things like Dropbox, Apple iCloud and Google Drive, which are simple and straightforward to use. There's no complicated scheduling or configuration compared to infrastructure backups. They make it easy for users to configure what files or folders they want to have backed up and then ensure the files are synchronized with what's stored in the cloud. As an IT support specialist, this is especially relevant. When users accidentally spill a cup of coffee on their laptop, they're going to come to you hoping their precious family photos can be saved. Getting users set up within easy to use and effective backup system for their files is great way to avoid this situation.

## Disaster recovery plans

### Whats a disaster recovery plan

We have all experienced an accident or made a mistake before. We're only human, right? As an IT support specialist, It's important that you're prepared for a disastrous accident or mistake. Maybe an electrical surge fried the hard drive in a database server or someone deleted the wrong folder. These things happen and you need to be prepared for them. This is where the disaster recovery plan comes in. A disaster recovery plan is a collection of documented procedures and plans on how to react and handle an emergency or disaster scenario, from the operational perspective. This includes things that should be done before, during and after a disaster. The goal of the disaster recovery plan is to minimize disruption to business and IT operations, by keeping downtime of systems to a minimum and preventing significant data loss. Despite the name, a disaster recovery plan will actually cover preventive measures and detection measures on top of the post disaster recovery approach. Preventative measures cover any procedures or systems in place that will proactively minimize the impact of a disaster. This includes things like regular backups and redundant systems. Anything that's done before an actual disaster that's able to reduce the overall downtime of the event is considered preventative. For example, a standard for critical network infrastructure or service to have redundant power supplies. They're often fed from different power sources like battery backup. This is designed to minimize the downtime that would be caused by one power supply failing or a power outage. That would be a preventative measure. We're going to some more detail on this in the next lesson, when we cover designing and effective disaster recovery plan. Detection measures are meant to alert you and your team that a disaster has occurred that can impact operations. Obviously, you need to be aware of a disaster in order to take appropriate steps to reduce the impact on your organization. Timely notification of a disaster is critical, since some steps of the disaster recovery plan might be time sensitive to ensure there is no data loss or equipment damage. If there a power outage for example, critical systems should fall back to battery power. But, battery backup power will only keep the systems on line for so long. To avoid potential data loss or damage, these systems should be gracefully shut down before they completely lose power. This is why lots of systems that support redundant power supplies also have a function to send alerts on power loss events. Other things that should be monitored to help head off any unexpected disasters include environmental conditions inside several networking rooms. Flood sensors can alert you to water coming into the server. Temperature and humidity sensors can watch for dangerously high temperatures or some optimal moisture levels in the air. This can alert you to failed cooling in the server room. Smoke detectors and fire alarms are also critically important. Remember, that it isn't just the technology that's necessary for a business to continue to operate. You also need the people working there. The specifics of building evacuation usually forward to the building management team, but as an IT support specialist, you'll likely work closely with some members of this team on things like, power delivery, heating and cooling systems and building evacuation. If there's a fire and the building needs to be evacuated, you should be prepared to set up temporary accommodation so people can still work effectively. This might be as simple as sending everyone home for the day and having them work from home. But you should be prepared for the situation ahead of time and have a plan in place to ensure that everyone is able to work from home effectively. Finally, corrective or recovery measures are those enacted after disaster has occurred. These measures involve steps like restoring lost data from backups or rebuilding and reconfiguring systems that were damaged. Once the disaster has been detected and steps have been taken to either prevent an outage or at least minimize downtime, work should begin on restoring full operations of everything affected. Usually, a disaster will take out one system that's part of a redundant pair or a replication scheme which would prevent a complete service outage. But that would mean you aren't prepared for another disaster. When one system in a redundant pair suffers a failure, it's called a single point of failure. This is because it only takes one failure now to completely take the system down. That's not a scenario you want to be in. We've covered the overall elements of a disaster recovery plan. Why don't you take a little break to recover yourself, then join me in the next video. We're going to run down the details of designing a disaster recovery plan of your own. Does that include planning for the zombie apocalypse? You have to watch to find out.

### Designing a disaster recovery plan

So, what exactly goes into an effective disaster recovery plan? Well, it depends. Keep in mind, there's no one-size-fits-all for disaster recovery plans. The mechanisms chosen and procedures put in place will depend a lot on the specifics of your organization and environment. But we can't start by covering the three types of measures in more detail. We'll also go over some examples to help give you an idea of what to think about. A good way to understand what to plan for is to perform a risk assessment. This involves taking a long hard look at the operations and characteristics of your teams. A risk assessment allows you to prioritize certain aspects of the organizations that are more at risk if there's an unforeseen event. Risk assessment can involve brainstorming hypothetical scenarios and analyzing these events to understand how they'd impact your organization and operations. When you look into preventive measures, pay attention to systems that lack redundancy. If it's something critical to permit operations, they should probably have a redundant spare, just in case. Make sure you have a sound backup and a recovery system, along with a good strategy in place. Ideally, you should have regular but automated backups to backup systems located both on site and off site. It's also critical that you have data recovery procedures clearly documented and kept up-to-date. Data recovery following a disaster is hopefully something you will rarely do. It's important to make sure that these procedures are updated since systems change and evolve throughout their lifetime. Redundancies shouldn't be limited only to systems. Anything critical to operations should be made redundant whenever possible. This includes power delivery or supply, communications systems, data links, and hardware. Think through the impacts that a disaster affecting each of these aspects would have on your day-to-day operations. What would happen to your network if the building lost power? Can you use continue to work at the fiber-optic data line if the building gets damaged by a nearby construction work? You call router for the office just burst into flames. Okay. The last one is a little far-fetched, but I think you get where I'm going. Another super important preventive measure that should be evaluated and verified is operational documentation. Make sure that every important operational procedure is documented and accessible. This includes things like setting up and configuring critical systems and infrastructure. Any steps or specific configuration details that are needed to restore 100 percent functionality to core systems and services should be documented in detail. It's also important that this documentation is kept up-to-date. An effective way to do this is periodically verify that the steps documented actually work. You don't want to find yourself in a situation where you need to reconfigure assistant following incident, only to discover that the documentation is wrong. When looking at detection measures, you'll want to make sure you have a comprehensive system in place that can quickly detect and alert you to service outages or abnormal environmental conditions. If up-time and availability is important for your organization, you'll likely have two internet connections; a primary and a secondary. You want to monitor the connection status of both of these links. Ideally, they should be configured to automatically fail over if one goes down. But you'll still want to be alerted when this happens, so you can investigate why the link went down and work on getting it back as soon as possible. The way to think about designing detection measures is to evaluate what's most critical to the day-to-day functioning of the organization. What infrastructure services and access are absolutely vital? Those are the ones you should be closely monitoring. And it's not just outages or complete failures you should be watching for. Of course, you want to monitor for those, but you also want to monitor for conditions that indicate that a problem is likely to occur. If we can avoid a catastrophic failure by being alerted to an overheating server before it fails, that would be much better, wouldn't it? So, you want to monitor conditions of service and infrastructure equipment. Things like temperatures, CPU load and network load for a service monitoring for error rates and requests per second will give you insight into the performance of the system. You should investigate any unusual spikes or unexpected increases. These early warning systems allow you to head off disaster before it brings operations to a halt. And of course, you absolutely must test these systems. Simulate the conditions your monitoring systems are designed to catch. Make sure the detection thresholds actually fire the alerts like they're supposed to. This testing goes beyond just the monitoring systems too. You'll also want to test your reactions and responses to these alerts. If you're monitoring systems reliably trigger alerts but everyone just ignores them, they aren't super useful, are they? You want to conduct regular disaster test to make sure systems are functioning and that your procedures to handle them are also up to the task. Corrective or recovery measures include actions that are taken to restore normal operations and to recover from an incident or outage. This includes taps like restoring a corrupted database from a backup or rebuilding and re-configuring a server. Your disaster plan should include reference or links to documentation for these types of tasks. Anything and everything that would be required to restore normal operations following some disaster. This is where the steps for restoring various systems and data from backups should be. The disaster recovery doc doesn't need to contain the details of the operations. Links and references are sufficient. But it's important to be prepared for a situation where typical documentation acts methods are unavailable. Let's imagine you keep all your operational documentation in a wiki on a dedicated server. What happens when that server suffers an outage? It's important that critical documentation is accessible if an emergency scenario or disaster strikes. In the next lesson, we'll cover what to do after a failure. See you there.

## Post mortems

### Whats a post mortem

Making mistakes is part of being human. We all make them from time to time, and hopefully each mistake is a learning opportunity. We look at what happened and try to understand why it did to avoid it in the future. Think of a toddler learning the stove is hot. They touch it once and it burns them. They quickly learn that touching the stove hurts, so they stop doing it. It's important that we're able to learn from our mistakes or else we'd constantly be burning ourselves. That's the purpose of a post-mortem report. We create a post-mortem after an incident, an outage, or some event when something goes wrong, or at the end of a project to analyze how it went. This report documents, in detail, what exactly happened leading up to, during, and after the event or project. It tries to highlight things that went well and things that didn't. The purpose of a post-mortem is to learn something from an event or project, not to punish anyone or highlight mistakes. Sure, they'll likely be some mistakes that'll be address but, the intention isn't to punish or shame, it's meant to understand the root cause of why the mistakes happen and how to prevent them from happening again. The post-mortem process isn't quite over yet, once the report is written up it needs to be communicated. These types of reports have value beyond the immediate people involved in the incident, investigation and writing of the report. Sharing post-mortems with other teams at an organization helps encourage a culture of learning from mistakes, it shows that your team is willing to acknowledge when you mess up. But you don't let mistakes hold you back, it sets a good example for others to follow and the content in the report might trigger the thought that some other team and make them realize they have a similar problem in their infrastructure. You may also identify areas that could be improved that are the responsibility of teams that weren't involved in the incident. When it comes to post-mortems, sharing is caring. If you embrace post-mortems, they tend to foster a culture where it's okay to make mistakes. This is a healthy attitude to have in any organization. If people are afraid to make mistakes, then decision making will be very conservative. It's hard to push the boundaries and try new things if everyone is afraid of screwing up. But if the prevailing culture says that mistakes are okay as long as we can learn from them, then you'll have an organization that's willing to take risks, and try out new and exciting ideas.

### Writing a post mortem

Now that we know the benefits of a postmortem, let's take a closer look at what goes into one. A typical postmortem for an incident begins with a brief summary, just a short paragraph, that summarizes the incident. It should include: what the incident was? How long it lasted? And what the impact was? And how it was fixed? Be mindful of time zone when listing times and dates in the postmortem. Always clearly state the time zone to be absolutely clear. Next, you need a detailed timeline of key events. This should include everything that happened throughout the event like when it started, and when people involved were notified or realized what was going on. Every action taken in an attempt to resolve this situation should also be identified. These could contain times and dates along with time zones, and who did what. The timeline should wrap up with the actions taken that resolved the outage and restored services, signaling the end of the event. Next, a very detailed and honest account of the root causes covered. This should go into detail explaining what led to the issue. It could be something like a configuration change that was pushed live without proper testing, or a command that was typoed. Remember that the intent isn't to blame or shame, is to be honest with what went wrong so that a lesson can be learned from it. If the cause stemmed from a lack of testing, this might indicate areas for improvement in test verification. If it was from a typoed command, this may reveal the need to automate a manual process. A more detailed explanation of the resolution and recovery efforts should be documented next. This is similar to the timeline covered earlier and should include the dates, times, and time zones. But it should go into more detail about what steps were taken to recover, the rationale and the reasoning behind those actions, and what the outcome of each that was including the rationale gives those reading the report more context on how the event played out. Lastly, close out the report with a list of specific actions that should be taken to avoid the same scenario from happening again. This should include any actions or efforts aimed at improving the response handling too. Steps to reduce response time when monitoring would help. When you spin up a list of things to improve, look out for things like improvements to monitoring systems. Maybe the incident investigation revealed a gap in visibility into critical systems, or the cause investigating turns out that automation system isn't functioning as intended. While it's outside the scope of a postmortem report to come up with solutions to these gaps, they should be listed in areas for improvement. Based on these discoveries, new parties can start to address the deficiencies found. One thing that often gets overlooked in postmortem is what went well. But this is just as important as analyzing what went wrong. During the post-incident analysis, it's also good to highlight things that went well. These include: fail safe or fail of a system that worked as designed, and prevented a large outage, or minimized the severity of the outage. This helps to demonstrate the effectiveness of our systems in place. For some folks, like those in finance, this is good news. It justifies any cost associated with these systems by clearly demonstrating a tangible benefit. This is important for any preventative system since they are frequently viewed as unnecessary costs by those that may not fully understand their benefit. These examples of systems working to prevent or reduce the impact of outages make that benefit very clear. Hopefully, you're better prepared now to learn from any mistakes you might make in your career. And mistakes will be made because you are human after all. Own them, learn from them, and do better next time. Such is true in IT, work, and in life. Well, that brings us to the close of our sysadmin course. We hope you have a better understanding of the responsibilities of a sysadmin, and how closely they relate to the work of an IT support specialist. Feel free to review any sections that might have been a bit heavy on the technical side. First up, we've brought a quiz for you that would touch on everything we've learned in this module. Then, when you're ready, you can jump into the course project to put your new knowledge to work. We have some fictional companies that you are going to play system administrator for. You need to take a look at their current infrastructure and make recommendations for improvements. I wish you the best of luck.