Google IT Support Specialization

Course 5: IT security

06 Creating a company culture for security

Table des matières

[1 Understanding IT security threat 2](#_Toc14416345)

[2 Pelcgbybtl cryptology 2](#_Toc14416346)

[3 AAA security not roadside assistance 2](#_Toc14416347)

[4 Securing your network 2](#_Toc14416348)

[5 Defense in depth 2](#_Toc14416349)

[6 Creating a company culture for security 2](#_Toc14416350)

[6.1 Risk in the workplace 2](#_Toc14416351)

[6.1.1 Security goals 2](#_Toc14416352)

[6.1.2 Measuring and assessing risk 3](#_Toc14416353)

[6.1.3 Privacy policy 4](#_Toc14416354)

[6.2 Users 5](#_Toc14416355)

[6.2.1 User habits 5](#_Toc14416356)

[6.2.2 Third party security 6](#_Toc14416357)

[6.2.3 Security training 7](#_Toc14416358)

[6.2.4 Alex grit story 7](#_Toc14416359)

[6.3 Incident handling 8](#_Toc14416360)

[6.3.1 Incident reporting and analysis 8](#_Toc14416361)

[6.3.2 Incident response and recovery 9](#_Toc14416362)

[6.3.3 Amir interview 10](#_Toc14416363)

[6.3.4 Ari interview 11](#_Toc14416364)

[6.4 Graded assessments 11](#_Toc14416365)

[6.4.1 Final assessment 11](#_Toc14416366)

[6.5 Course wrap up 11](#_Toc14416367)

[6.5.1 Congratulations 11](#_Toc14416368)

# Understanding IT security threat

# Pelcgbybtl cryptology

# AAA security not roadside assistance

# Securing your network

# Defense in depth

# Creating a company culture for security

## Risk in the workplace

### Security goals

Congratulations. You've reached the last chunk of the last course of this program. You are totally ready to lock down every single operation of your organization and make it airtight. Right? Not quite. If you're responsible for an organization of users, there's a delicate balance between security and user productivity. We've seen this balance in action when we dove into the different security tools and systems together. Before you start to design a security architecture, you need to define exactly what you like it to accomplish. This will depend on what your company thinks is most important. It will probably have a way it wants different data to be handled and stored. You also need to know if your company has any legal requirements when it comes to security. If your company handles credit card payments, then you have to follow the PCI DSS or Payment Card Industry Data Security Standard depending on local laws. We'll take a closer look at PCI DSS which is a great example of clearly defined security goals. PCI DSS is broken into six broad objectives, each with some requirements. The first objective is to build and maintain a secure network and systems. This includes the requirements to install and maintain a firewall configuration to protect cardholder data and to not use vendor supply default for system passwords and other security parameters. As you can tell, the requirements are related to the objective. The objective is the end goal or what we'd like to achieve and the requirements are the actions that can help achieve that goal. PCI DSS goes into more detailed actions for each requirement. It provides more specific guidance around what a firewall configuration should control. For example, a secure firewall configuration should restrict connections between untrusted networks and any systems in the cardholder data environment. That's a little generic, but it does give us some guidance on how to meet the requirements. The second objective category is to protect cardholder data. In this objective, the first requirement is to protect stored cardholder data. The second is to encrypt the transmission of cardholder data across open public networks. I want to call out again how the broad objective is to protect sensitive data that's stored in systems within our control. The requirements give us specific guidelines on how to get this done. The specifics of these requirements help clarify some of the points like what constitutes an open network. They also recommend using strong cryptography and offer some examples. But not all requirements are technical in nature. Let's look at the requirement to protect stored cardholder data for example, it has requirements for data retention policies to make sure that sensitive payment information isn't stored beyond the time it's required. Once payment is authorized, authentication data shouldn't be needed anymore and it should be securely deleted. This highlights the fact that good security defenses aren't just technical in nature. They are also procedural and policy-based. The third objective is to maintain a vulnerability management program. The first requirement is to protect all systems against malware and regularly update antivirus software or programs. The second is to develop and maintain secure systems and applications. You'll find more detailed implementation procedures within these requirements. They'll cover things like ensuring all systems have antivirus software installed and making sure this software is kept up to date. They also require that scans are run regularly and logs are maintained. There are also requirements for ensuring systems and software are protected against known vulnerabilities by applying security patches at least one month from the release of a security patch. Use of third-party security vulnerability databases is also listed to help identify known vulnerabilities within managed systems. The fourth objective is to implement strong access control measures. This objective has three requirements. The first is to restrict access to cardholder data by business need-to-know. The second is to identify and authenticate access to system components. And the third is to restrict physical access to cardholder data. This highlights the importance of good access control measures along with good data access policies. The first objective, restricting access to data by business need-to-know, means that any sensitive data should be directed to data access policies to make sure that customer data isn't misused. Part of this requirement is to enforce password authentication for system access and two factor authentication for remote access, that's the minimum requirement. Another important piece highlighted by the PCI DSS requirements is access control for physical access. This is a critical security aspect to keep in mind since we need to protect systems and data from both physical theft and virtual attacks. The fifth objective is to regularly monitor and test networks. The first requirement is to track and monitor all access to network resources and cardholder data. The second is to regularly test security systems and processes. The requirement for network monitoring and testing is another essential part of a good security plan. This refers to things like setting up and configuring intrusion detection systems and conducting vulnerability scans of the network which will cover a bit more later. Testing defenses is another super important part of this. Just having the systems in place isn't enough. It's really helpful to test defense systems regularly to make sure that they provide the protection that you want. It also ensures that the alerting systems are functional. But don't worry, we'll dive deeper into this a little bit later when we cover penetration testing. The sixth and final objective is to maintain an information security policy. It only has one requirement, to maintain a policy that addresses information security for all personnel. This requirement addresses why we need to have well-established security policies. They help govern and regulate user behavior when it comes to information security aspects. It's important to call out that this requirement mentions that the policy should be for all personnel. The responsibility of information security isn't only on the security teams. Every member of an organization is responsible for information security. Well-designed security policies address the most common questions or use cases that users would have based on the specific details of the organization. Every one that uses systems on your organization's network, is able to get around security. They might not mean to, but they can reduce the overall security with their actions and practices. That's why having well-thought-out security policies in place also need to be easy to find, and easy to read. We'll cover more details about user education and getting users involved in the overall security plan in another upcoming video of this course.

### Measuring and assessing risk

We've covered Security Risk Assessment a little bit in the last lesson. But there's lots more to talk about. Security is all about determining risks or exposure understanding the likelihood of attacks; and designing defenses around these risks to minimize the impact of an attack. This thought process is actually something that everyone uses in their daily life, whether they know it or not. Think of when you cross a busy intersection, you assess the probability of being hit by an oncoming car and the minimize that risk by choosing the right time to cross the road. Security risk assessment starts with threat modeling. First, we identify likely threats to our systems, then we assign them priorities that correspond to severity and probability. We do this by brainstorming from the perspective of an outside attacker putting ourselves in a hackers shoes. It helps to start by figuring out what high value targets an attacker may want to go after. From there, you can start to look at possible attack vectors that could be used to gain access to high value assets. High-value data usually includes account information, like usernames and passwords. Typically, any kind of user data is considered high value, especially if payment processing is involved. Another part of risk measurement is understanding what vulnerabilities are on your systems and network. One way to find these out is to perform regular vulnerabilities scanning. There are lots of open source and commercial solutions that you can use. They can be configured to perform scheduled, automated scans of designated systems or networks to look for vulnerabilities. Then they generate a report. Some of these tools are Nessus, OpenVas and Qualys which I've linked to in the next reading. Let me break down what vulnerability scanners do. Heads up, this might be a little dense, so feel free to go over it again. Vulnerability scanners are services that run on your system within your control that conduct periodic scans of configure networks. The service then conducts scans to find and discover hosts on the network. Once hosts are found either through a ping sweep or port scanning more detailed scans are run against discovered hosts scans, upon scans, upon scans. A port scan of either common ports or all possible valid ports is conducted against discovered hosts to determine what services are listening. These services are then probed to try to discover more info about the type of service and what version is listening on the relevant port. This information can then be checked against databases of known vulnerabilities. If a vulnerable version of a service is discovered, the scanner will add it to its report. Once the scan is finished the discovered vulnerabilities and hosts are compiled in a report, that way and analysts can quickly and easily see where the problem areas are on the network. Found vulnerabilities are prioritized according to severity, and other categorization. Severity takes into account a number of things, like how likely the vulnerability is to be exploited. It also considers the type of access the vulnerability would provide to an attacker and whether or not it can be exploited remotely or not. Vulnerabilities and the report will have links to detailed and disclosed information about the vulnerability. In some cases, it will also have recommendations on how to get rid of it. Vulnerability scanners will detect lots of things, ranging from misconfigured services that represent potential risks, to detecting the presence of back doors and systems. It's important to call out that vulnerability scanning can only detect known and disclose vulnerabilities and insecure configurations. That's why it's important for you to have an automated vulnerability scan conducted regularly. You'll also need to keep the vulnerability database up to date, to make sure new vulnerabilities are detected quickly. But vulnerability scanning isn't the only way to put your defenses to the test. Conducting regular penetration tests is also really encouraged to test your defenses even more. These tests will also ensure detection and alerting systems are working properly. Penetration Testing is the practice of attempting to break into a system or network to verify the systems in place. Think of this as playing the role of a bad guy, for educational purposes. This exercise isn't designed to see if you have the acting chops it's intended to make you think like an attacker and use the same tools and techniques they would use. This way, you can test your systems to make sure they protect you like they're supposed to. The results of the penetration testing reports will also show you, where weak points or blind spots exist. These tests help improve defenses and guide future security projects. They can be conducted by members of your in-house security team. If your internal team doesn't have the resources for this exercise you can hire a third party company that offers penetration testing as a service. You can even do both. That would help give you more perspectives on your defense systems and you'll get a more comprehensive test this way.

### Privacy policy

When you're supporting systems that handle customer data, it's super important to protect it from unauthorized and inappropriate access. It's not just to defend against external threats, it also protects that data against misuse by employees. This type of behavior would fall under your company's privacy policies. Privacy policies oversee the access and use of sensitive data. They also define what appropriate and authorize use is, and what provisions or restrictions are in place when it comes to how the data is used. Keep in mind that people might not consider the security implications of their actions, so both privacy and data access policies are important to guiding and informing people how to maintain security while handling sensitive data. Having defined and well established privacy policies is an important part of good privacy practices. But you also need a way to enforce these policies. Periodic audits on cases where sensitive data was accessed can get you there. This was enabled by our logging and monitoring systems. Auditing data access logs is super important, it helps us ensure that sensitive data is only accessed by people who are authorized to access it, and that they use it for the right reasons. It's good practice to apply the principle of least privilege here, by not allowing access to this type of data by default. You should require anyone that needs access to first make an access request with a justification for getting the data. But it can't just be vague or generic requests for access, they should be required to specify what data they need access to. Usually, this type of request would also have a time limit that should be called out in a request. That way, you can ensure that data access is only permitted for legitimate business reasons which reduces the likelihood of inappropriate data access or usage. By logging each day the access request and actual data access, we can also correlate requests with usage. Any access that doesn't have a corresponding request should be flagged as a high-priority potential breach that needs to be investigated as soon as possible. Company policies act as our guidelines in informational resources on how and how not to access and handle data. They're equally important here. Policies will range from sensitive data handling to public communications. Data handling policies should cover the details of how different data is classified. What makes some data sensitive as opposed to non sensitive? What's considered confidential data? Well, once different data classes are defined, you should create guidelines around how to handle these different types of data. If something is considered sensitive or confidential, you probably have stipulations that this data shouldn't be stored on media that's easily lost or stolen, like USB sticks or portable hard drives. They're also commonly used without any encryption at all. Imagine if one of your employees lost an unencrypted portable hard drive full of customer information, disaster. That's exactly the situation a data access policy tries to avoid. It might also make sense to include laptops and mobile devices, like phones and tablets in the removable media classification, since these devices are easily lost or stolen. Even though they're more commonly encrypted these days, the loss and theft rate is much higher. You may not like users storing sensitive data on a removable media, but sometimes you're out of luck. There may be an occasion where that's the only solution to accomplish a task. If this is the case, it would help to have recommendations on how to handle the situation in a secure way. So, you could offer an appropriate encryption solution, and provide instructions, and support on its use.

## Users

### User habits

You've got to involve your users when it comes to security. It's super important and might seem obvious, but it's usually overlooked. You can build the world's best security systems, but they won't protect you if the users are going to be practicing unsafe security. If a user writes their password on a post-it note, sticks it to their laptop, then leaves the laptop unlocked and unattended at a cafe, you could have a disaster on your hands. But making sure that your users take reasonable security precautions takes effort and can be really tricky. You have to make sure your users habits and actions involve having clear and reasonable security policies. But there's more that you can do to help ensure that your users are diligent about maintaining security. Let's assume that your employees are acting with good intent, and that leaks and disclosures are unintentional, and mostly due to improper handling of sensitive data. Leaks and disclosures can be avoided by understanding what employees need to do to accomplish their jobs. You also need to make sure that they have the right tools to get their work done without compromising security. If an employee needs to share a confidential file with an external partner and it's too big to e-mail, they may want to upload it to a third-party file sharing website that they have a personal account with. This is risky business. You should never upload confidential information onto a third-party service that hasn't been evaluated by your company. If sharing big files with external parties is common behavior for your employees, it's best to find a solution that meets the needs of your users and the security guidelines. By providing a sanctioned and approved mechanism for this file sharing activity, users are less likely to expose the organization to unnecessary risk. We covered password security when we discussed password authentication earlier, but there's more to talk about when it comes to users and passwords. I hate to say it, but generally speaking, users can be lazy about security stuff. They don't like to memorize long complicated passwords, but this is super important to keeping your company safe. So how do we resolve this conflict. If we require 20 character passwords that have to be changed every three months, our users will almost definitely write them down. This compromises the security that our complex password policy is supposed to provide. It's important to understand what threats password policies are supposed to protect against, that way, you can try to find a better balance between security and usability. A long and complex password requirement is designed to protect against brute force attacks, either against authentication systems or if a hashed password database is stolen. Since direct brute force attacks against authentication infrastructure should be easily detected and blocked by intrusion prevention systems, they can be considered pretty low risk. But the theft of a password database would be a super serious breach. We do have lots of additional layers of security in place to prevent a critical compromise like that from happening in the first place. So the two attacks that complex passwords are primarily designed to protect against, are fairly low risk. Now, we can relax the password requirements a bit and not ask for overly long passwords. We can even adjust the mandatory password rotation time period. Password reuse is another common user behavior. People don't want a bunch of passwords to memorize, lots of users find it easier to use the same password, for both their personal email account and their work account. But this undermines the security of their work password. If an online service is compromised and the password database is leaked, they're in trouble. The passwords in that database will find their way into password files used for cracking passwords and brute force attacks. Once a password isn't a secret, it shouldn't be used anymore. The chances of a bad actor being able to use the password are too high. That's why it's important to make sure employees use new and unique passwords, and don't reuse them from other services. It's also important to have a password change system check against old passwords. This will prevent users from changing their password back to a previously used potentially compromised password. A much greater risk in the workplace that users should be educated on is credential theft from phishing emails. Phishing emails are pretty effective. They take advantage of people's inclination to open emails without looking at them too closely. If an e-mail that seems authentic actually leads to a fake login page, users can blindly enter their credentials into the fake site and disclose their credentials to an attacker. While having two factor authentication helps protect against this type of attack, OTP-based two factor solutions would still provide usable credentials to an attacker, plus the attacker still has a password which is really not good even in a two factor environment. If someone entered their password into a phishing site or even suspects they did, it's important to change their password as soon as possible. If you can, your organization should try to detect these types of password disclosures using tools like password alert, which I've linked to in the next reading. This is a Chrome extension from Google that can detect when you enter your password into a site that's not a Google page. Being able to detect when a password is entered into a potentially untrustworthy site, lets an organization detect potential phishing compromises. But you can also combat phishing attacks with good spam filtering combined with good user education. You can help influence good user behavior by offering security training, which we'll discuss in another video. Next up, we'll do a quick rundown of the benefits and tradeoffs of third-party security. I'll see you there.

### Third party security

Sometimes, you need to rely on third party solutions, or service providers, because you might not be able to do everything in-house. This is especially true if you work as an IT support specialist in a small shop. In some cases, you'll have to trust that third party with a lot of potentially-sensitive data or access. So, how do you make sure that you aren't opening yourself up to a ton of unnecessary risk? When you contract services from a third party, you're trusting them to protect your data and any credentials involved. If they have sub par security, you're undermining your security defenses by potentially opening a new avenue of attack. It's important to hire trustworthy and reputable vendors whenever you can. You also need to manage the engagements in a controlled way. This involves conducting a vendor risk review or security assessment. In typical vendor security assessments, you ask vendors to complete a questionnaire that covers different aspects of their security policies procedures and defenses. The questionnaire is designed to determine whether or not they've implemented good security designs in their organization. For software services, or hardware vendors, you might also ask to test the software/ hardware, that way, you can evaluate it for potential security vulnerabilities or concerns before deciding to contract their services. It's important to understand how well-protected your business partners are, before deciding to work with them. If they have poor security practices, your organization's security could be at risk. If you contract services from a company that will be handling data on your behalf, the security of your data is in the hands of this third party. It's important to understand how safe your data will be with them. Sometimes, vendors will perform tasks for you, so they'll have access to your network and systems. In these cases, it's also important to understand how well secured third party is. A compromise of their infrastructure could lead to a breach of your systems. While the questionnaire model is a quick way to assess a third party, it's not ideal. It depends on self reporting of practices, which is pretty unreliable. Without a way to verify or prove what's stated in the questionnaire, you have to trust that the company is answering honestly. While you'd hope that a company you're doing business with would be honest, it's best to verify. If you can, ask for a third party security assessment report. Some of the information on the questionnaire can be verified, like third party security audit results and penetration testing reports. In the case of third party software, you might be able to conduct some basic vulnerability assessments and tests to ensure the product has some reasonable security. There are lots of companies that will evaluate vendors for you for a price. But, Google recently made their vendor security assessment questionnaires available for free. I provided a link to these questionnaires just after this video. That's a great starting point to design your own vendor security assessment questionnaire, or you can just use these as is. If the third party service involves the installation of any infrastructure equipment on site, pay close attention to how they're doing it. You have to make sure this equipment's managed in a way, that doesn't negatively affect overall security. Let's say, the vendor company requires remote access to the infrastructure device to perform maintenance. If that's the case, then make appropriate adjustments to firewall rules to restrict this access. That way, you'll make sure that it can't be used as an entry point into your network. Additional monitoring would also be recommended for this third party device since it represents a new potential attack surface in your network. If the vendor lets you, evaluate the hardware in a lab environment first. There, you can run in-depth vulnerability assessments and penetration testing of the hardware, and make sure there aren't any obvious vulnerabilities in the product. Report your findings to the vendor and ask that they address any issues you discover.

### Security training

The more trained up you and your colleagues are on security, the better. It's impossible to have good security practices at your company if employees and users haven't received good trainings and resources. This will boost a healthy company culture and overall attitude toward security. A working environment that encourages people to speak up when they feel something isn't right is critical, it encourages them to do the right thing. To help create this context, it's important for employees to have a way that they can ask questions when they come up. This could be a mailing list where users can ask questions about security concerns or to report things they suspect are security risks. Having the designated communication channel where people can feel comfortable asking questions and getting clear answers back is super important. Helping others keep security in mind will help decrease the security burdens you'll have as an I.T. Support Specialist. It will also make the overall security of the organization better. Creating a culture that makes security a priority isn't easy. You have to reinforce and reward behaviors that boost the security of your organization. Think of the small things we do every day when we use our computers. Just entering your password to login or locking your screen when you walk away from your computer is helpful. Hopefully, you're careful about entering your password on websites and check the address of the site you're authenticating against. If you aren't, try it out to avoid entering your password into a fake website. When you're working on your laptop in a public space, like a library or coffee shop, do you lock your screen when you leave to use the restroom or get another caffeine fix? If not, you absolutely should be. Hopefully, you weren't leaving your computer unattended in public, in the first place. That's a really bad idea. These are the types of small things that security training should address. You also need to justify why these are good behaviors to adopt. In some cases, the company culture can turn screen locking into a sort of game. When colleagues forget to lock their screen, other team members can play harmless pranks on them. The last time I forget to lock my computer, my colleague change the default language to Turkish. It reminded me to always lock my screen, because anyone with access to the machine can impersonate you and get access to any resources you're logged into. But building a culture that embraces security principles isn't always enough. There are some things that all employees should know. This is when an occasional, mandatory, or security training course can help. This could be a short video or informational presentation followed by a quiz to see if your employees understood the key concepts covered in the training. The quiz can also increase the chances of information being retained. Making employees retake the training every once a year or so, ensures that everyone's up-to-date on their training. You can also cover new concepts or updated policies when needed. This type of training should cover the most common attack types and how to avoid falling victim to them. This includes things like phishing emails and best practices around password use. These trainings often include scenarios that can help test the user's understanding of a particular topic. Training courses like these are the last in the line of defenses that you and your company need to have in place to make sure that you're as safe as possible, for as long as possible.

### Alex grit story

To have a successful career in IT, there are several things that are needed. Tenacity, grit, being able to solve challenging problems, again not having all the technology solve it but knowing how to get there. And, for me a great IT support candidate, or a great IT candidate- but somebody that is not afraid to make mistakes. Is having that tenacity, being able to deal with some of the downsides because that is a big part of it, is the learning part of it, that ability to look at something and say, "Okay, this is something, even though it seems insurmountable, it seems huge, I can attack this in whatever degree, small degrees and fix it." Very early on I was interviewing for techs many years ago. We worked in a small space in downtown Ann Arbor and there was an alleyway in the back of our office and, we had a fire escape. We were on the second floor of this office and there was this fire escape leading up. And, I was waiting for an interview candidate to come in, somebody I'd never met before. The receptionist comes up to me a few minutes later and tells me that the interview candidate was here. And, I sat down with the person and I said, "Are you the person that was escorted in a few minutes ago from the back?" And he says, "Yeah." What had happened was, he couldn't find the entrance to the building. Very, very complicated. Very weird. It was an odd building. It wasn't well-marked. The doors were hard to find, a lot of people ran into that. So, went around back to this squishy alleyway. He was in a suit coming in for an interview. He climbed this rusty old fire escape, banging on the back door to get in. And, that had me sold right from the beginning. I'm like [inaudible] a problem. Regardless of whether or not he was going to be a little bit dirty or sweaty or whatever, he found a way to solve it. And that's really what I look for, for that level of tenacity where even if they struggled, sometime I prefer that. This was hard for me but I got through it and I was successful in the end. That's what I look for.

## Incident handling

### Incident reporting and analysis

We try our best to protect our systems and networks. But it's pretty likely that some sort of incident will happen. This could be anything from a full system compromise and data theft, to someone accidentally leaking a memo. Regardless of the nature of the incident, proper incident handling is important to understanding what exactly happened, and how it happened and how to avoid it from happening again. The very first step of handling an incident is to detect it in the first place. Hopefully, our intrusion detection systems caught the telltale signs of an ongoing attack, and alerted us to the threat. Incidents can be brought to your attention in other ways too. An employee may have noticed something suspicious and reported it to the security team for investigation, or maybe they leaked information that ended up in the news. However, you found out about the incident. The next step is to analyze it and determine the effects and scope of damage. Was it a data leak? Or information disclosure? If so, what information got out? How bad is it? Were systems compromised? What systems? And what level of access did they manage to get? Is it a malware infection, what systems were infected? Some attacks are really obvious with very clear signs of an intrusion like a defaced webpage or unusual process consuming all resources in the system. Others may be way more subtle and almost impossible to detect, like a small change to a single system configuration file. This is why having good monitoring in place is so important along with understanding your baseline. Once you figure out what normal traffic looks like on your network and what services you expect to see, outliers will be easier to detect. This is important because every false lead that the incident response team has to investigate means time and resource is wasted. This has the potential to allow real intrusions to go undetected and uninvestigated longer. During detection and scoping, correlating data from different systems can reveal a much bigger picture of what's happened. It might show how an intruder gained access. For example, you could see a connection event logged by the firewall from a suspicious IP address, searching for other events related to this IP address may reveal logging attempts and the authentication logs for a system. This would provide insight into where the attacker is coming from and what they attempted to do on the network. The authentication logs would also indicate, whether or not they were able to successfully log into an account. If so, that's lets you know what account is compromised. Once the scope of the incident is determined, the next step is containment. You need to contain the breach to prevent further damage. For system compromises and malware infection, this is a pretty time sensitive step. You don't want the malware or attacker to use one compromised machine to pivot to other machines inside your network. This could broaden the incidence scope and cause even more damage. Containment strategies will vary depending on the nature of the incident. If an account was compromised, change the password immediately. If the owner is unable to change the password right away, then lock the account. Also, revoke any long-lived authentication tokens, since the attacker may have one of those too. If it's a malware infection, can our anti-malware software quarantine? Or remove the infection? If not, the infected machine needs to be removed from the network as soon as possible to prevent lateral movement around the network. To do this, you can adjust network-based firewall rules to effectively quarantine the machine. You can also move the machine to a separate VLAN used for security quarantining purposes. This would be a VLAN with strict restrictions and filtering applied to prevent further infection of other systems and networks. It's important during this phase that efforts are made to avoid the destruction of any logs or forensic evidence. Attackers will usually try to cover their tracks by modifying logs and deleting files, especially when they suspect they've been caught. They'll take measures to make sure they keep their access to compromised systems. This could involve installing a backdoor or some kind of remote access malware. Another step to watch out for is creating a new user account that they can use to authenticate within the future. With effective logging configurations and systems in place, these activities would show up in audit logs. So this type of access should be detected during an incident investigation, then actions can be taken to remove access. I hope I'm not scaring you with all these scenarios, but it's better to be safe than sorry. Another part of incident analysis is determining severity, impact, and recoverability of the incident. Severity includes factors like what and how many systems were compromised and how the breach affects business functions. An incident that's compromised a bunch of machines in the network would be more severe than one where a single web server was hacked, for example. You can imagine that the effort required to fix a large scale compromise would negatively affect the ability to do normal work. So, the impact of an incident is also an important issue to consider. If the organization only had one web server and it was compromised, it might be considered a much higher severity breach. It would probably have a direct externally visible impact on the business. Data exfiltration, is the unauthorized transfer of data from a computer. It's also a very important concern when a security incident happens. Hackers may try to steal data for a number of reasons. They may want to steal account information to provide access later. They may target business data to publish online to cause financial loss or damage to the organization's reputation. In some cases, the attacker may just want to cause damage and destruction, which might involve deleting or corrupting data. What actions have been taken will affect the recoverability of the incident? The recoverability is how complicated and time-consuming the recovery effort will be. An incident that can be recovered with a simple restoration from backup by following documented procedures would be considered easily recovered from. But, an incident where an attacker deleted large amounts of customer information and wrecked havoc across lots of critical infrastructure systems would be way more difficult to recover from. It might not be possible to recover from it at all. In some cases, depending on backup systems and configurations, some data may be lost forever and can't be restored. Backups won't contain any changes or new data that were made after the last backup run.

### Incident response and recovery

Once a threat has been detected and contained, it has to be removed or remediated. When it comes to malware infection, this means removing the malware from affected systems. But in some cases, this may not be possible, so the affected systems have to be restored to a known good configuration. This can be done by rebuilding the machine or restoring from backup. Take care when removing malware from systems because some malware is designed to be very persistent, which means it's resistant to being removed. But before we can start the recovery, we have to contain the incident. This might involve shutting down affected systems to prevent further damage or spread of an infection. On the flip side of that, affected systems may just have network access removed to cut off any communication with the compromised system. Again, the motivating factor here would be to prevent the spread of any infection or to remove remote access to the system. The containment strategy varies depending on the nature of the affected system. Let's say a critical piece of networking infrastructure was compromised. A quick shutdown may not work since it would impact other business operations. On top of that, removing networking access might trigger fail safes in attack software or malware. Let's say a piece of malware is designed to periodically check into a command and control server. Severing network communications with the infected host might cause the malware to trigger a self destruct function in an attempt to destroy evidence. Forensic analysis may need to be done to analyze the attack. This is especially true when it comes to a malware infection. In the case of forensic analysis, affected machines might be investigated very closely to determine exactly what the attacker did. This is usually done by taking an image of the disk, essentially making a virtual copy of the hard drive. This lets the investigator analyze the contents of the disk without the risk of modifying or altering the original files. If that happened, it would compromise the integrity of any forensic evidence. Usually, evidence gathering is also part of the incident response process. This provides evidences to law enforcement if the organization wants to pursue legal action against the attackers. Forensic evidence is super useful for providing details of the attack to the security community. It allows others security teams to be aware of new treats and lets them better defends themselves. It's also very important that you get members from your legal team involved in any incident handling plans. Because an incident can have legal implications for the company, a lawyer should be available to consult and advise on the legal aspects of the investigation. It's crucial in order to avoid complications or issues of liability. Members of the public relations team should also get involved since these incidents can have an impact on a company's reputation. There is another part of the cleanup and recovery phase I should call out. We'll need to use information from the analysis to prevent any further intrusions or infections. First, we determine the entry point to figure out how the attacker got in, or what vulnerability the malware exploited. This needs to be done at the same time as the cleanup. If you remove the malware infection without also addressing the underlying vulnerability, systems could become reinfected right after you clean them up. As you learned in the system administration and IT infrastructure services course, postmortems can be a great way to document incidents. The learnings from postmortems can be used to prevent those incidents from happening again. If a critical system has been compromised, remediation can be complicated because of downtime during remediation and recovery. Logs have to be audited to determine exactly what the attacker did while they had access to the system. They'll also tell you what data the attacker accessed. Systems must be scrutinized to ensure no back doors have been installed, or malware planted on the system. Depending on the severity of the compromise or infection, it might be necessary to rebuild the system from the ground up. Cleanup would typically involve restoring from a backup point to a known good configuration. Infected or corrupted system files could be restored from known good copies. Sometimes, cleanup can be very simple and quick. I hope that's what you find more often than not. If a website was defaced, the attacker may have simply uploaded their defaced HTML file and pointed the web server at the new file. A configuration file change and deletion of the attacker's HTML file would undo those changes. Even so, efforts need to be made to determine how the attacker got access. That vulnerability should be closed to prevent any future attacks. When all traces of the attack have been removed and discovered and the known vulnerabilities have been closed, you can move on to the last step. That's when systems need to be thoroughly tested to make sure proper functionality has been restored. Usually, affected systems would also remain under close watch, sometimes with additional detailed monitoring and logging enabled. This is to watch for any additional signs of an intrusion in case something was missed during the cleanup. It's also possible that the attacker will attempt to attack the same target again. There's a very high chance that they use the same or similar attack methodology on other targets in your network. It's important to incorporate the lessons you've learned from any incident into your overall security defenses. Update firewall rules and ACLs if an exposure was discovered in the course of the investigation. Create new definitions and rules for intrusion detections systems that can watch for the signs of the same attack again. Stay vigilant and prepared to protect your system from attacks. Remember that at some point, some sort of security breach will happen. Just stay calm and execute your plan to counterattack the breach.

### Amir interview

[MUSIC] The typical interview for IT support candidate is going to be some form of role playing. Are you able to communicate with a wide range of individuals? Are you able to communicate very difficult concepts to people who may not have such a strong technical background? Often they will use past examples of real life situations and role play those with you in the interview. And they want to see how you handle that, especially if they throw in someone who's had a really bad day and comes to you with the problem that was the last straw that broke the came's back. They want to see if your approach is just the brute force method to solve the problem. Or if you're taking a creative, efficient approach to solving something, all while doing this with a positive attitude and leaving the user feeling empowered to solve these problems for them self in the future. It can help to practice in person, practice over the phone, practice over a video, because in today's world, you're supporting people on all three mediums. So each one will have a little tweak of how soft skills can play a big role in the relationship you have with the user. [MUSIC]

### Ari interview

[MUSIC] It's very important to do prior research on the role of the company that you're interviewing for. You want to make sure that you have some questions in advance prepared for your interviewer on those two things. So in terms of the role, feel free to ask your interviewer their perspective on the day to day of what you'll be doing. In terms of asking questions about the company, you want to show that you have some of the same values and mission that the company has in asking questions along those lines. Outside of soft skills, some of the qualities that a hiring manager or an interviewer may be looking for are going to be are you showing that you have a methodical approach to the way that you're approaching the problem? Another quality that hiring managers or interviewers may be looking for is the ability to problem solve. IT professionals are not going to know everything about IT. But you do want to show that you are able to think on the spot, challenge yourself, and still walk through a scenario even if it is a bit unfamiliar to you. In order to prepare for the troubleshooting and problem-solving aspect of the interview, a good way to do that is to practice via mock interviews. So that you do get in the art and the exercise of being able to walk out and talk out your thought process. Find yourself a person that can run through some questions with you. Whether that be a roommate, a relative, identify some questions that they can ask you. Real life scenario questions that you've either encountered or haven't encountered before, and have them ask those questions. Practice walking out something that you're not as familiar with. And practice your communication skills in delivering that, even if you're not sure of the answer. [MUSIC]

## Graded assessments

### Final assessment

Wow. You've made it to the final project of the final course. You are almost there. After weeks and months of hard work, you've nearly reached the end of this program. Best of luck on your final assignment. We have no doubt you'll shine considering how much you've accomplished so far. Stay focused and I'll be there to congratulate you at the end.

## Course wrap up

### Congratulations

Congratulations on all you've accomplished. What you have achieved is no small feat. It's very difficult to dive into a topic that you know nothing about from the very beginning to become the expert that you are now. That you've done a lot of work. It's been an incredible journey. These are all not easy concepts to get, but you made it through the whole thing. It's an amazing accomplishment and you should be really proud of yourself. Congrats, that's great work. Congratulations. Congratulations. Congratulations. Congratulations. Congratulations. Congratulations. You're probably exhausted right now, but congratulations and I hope that all this was super exciting and that you're really excited about where you can take this now. Congratulations, you've made it through the program. Now get out there and get a job and get your career started.