Module 1 - Protect data and communicate incidents

Data and asset classification

Protecting an organization’s business operations and assets from security threats, risks, and vulnerabilities is important. You previously learned what it means to have a security mindset. That mindset can help you identify and reduce security risks and potential incidents.
In this reading, you will learn about key data classification types and the difference between the low-level and high-level assets of an organization.

Classifying for safety

Security professionals classify data types to help them properly protect an organization from cyber attacks that negatively impact business operations. Here is a review of the most common data types:

- **Public data**
- **Private data**
- **Sensitive data**
- **Confidential data**

Public data

This data classification does not need extra security protections. **Public data** is already accessible to the public and poses a minimal risk to the organization if viewed or shared by others. Although this data is open to the public, it still needs to be protected from security attacks. Examples of public data include press releases, job descriptions, and marketing materials.

Private data

This data classification type has a higher security level. **Private data** is information that should be kept from the public. If an individual gains unauthorized access to private data, that event has the potential to pose a serious risk to an organization.
Examples of private data can include company email addresses, employee identification numbers, and an organization’s research data.

Sensitive data

This information must be protected from everyone who does not have authorized access. Unauthorized access to sensitive data can cause significant damage to an organization’s finances and reputation.
Sensitive data includes personally identifiable information (PII), sensitive personally identifiable information (SPII), and protected health information (PHI). Examples of these types of sensitive data are banking account numbers, usernames and passwords, social security numbers (which U.S. citizens use to report their wages to the government), passwords, passport numbers, and medical information.

Confidential data

This data classification type is important for an organization’s ongoing business operations. **Confidential data** often has limits on the number of people who have access to it. Access to confidential data sometimes involves the signing of non-disclosure agreements (NDAs)— legal contracts that bind two or more parties to protect information—to further protect the confidentiality of the data.

Examples of confidential data include proprietary information such as trade secrets, financial records, and sensitive government data.

Asset classification

Asset classification means labeling assets based on sensitivity and importance to an organization. The classification of an organization's assets ranges from low- to high-level. Public data is a low-level asset. It is readily available to the public and will not have a negative impact on an organization if compromised. Sensitive data and confidential data are high-level assets. They can have a significantly negative impact on an organization if leaked publicly. That negative impact can lead to the loss of a company's competitive edge, reputation, and customer trust. A company's website address is an example of a low-level asset. An internal email from that company discussing trade secrets is an example of a high-level asset.

Disaster recovery and business continuity

The role of a security professional is to ensure a company's data and assets are protected from threats, risks, and vulnerabilities. However, sometimes things don't go as planned. There are times when security incidents happen. You've already learned that security breaches can lead to financial consequences and the loss of credibility with customers or other businesses in the industry.

This reading will discuss the need to create business continuity and disaster recovery plans to minimize the impact of a security incident on an organization's business operations. Analysts need to consider the sequence of steps to be taken by the security team before business continuity and disaster recovery plans are implemented.

Identify and protect

Creating business continuity and disaster recovery plans are the final steps of a four-part process that most security teams go through to help ensure the security of an organization. First, the security team identifies the assets that must be protected in the organization. Next, they determine what potential threats could negatively impact those assets. After the threats have been determined, the security team implements tools and processes to detect potential threats to assets. Lastly, the IT or appropriate business function creates the business continuity and disaster recovery plans. These plans are created in conjunction with one another. The plans help to minimize the impact of a security incident involving one of the organization's assets.

Business continuity plan

The impact of successful security attacks on an organization can be significant. Loss of profits and customers are two possible outcomes that organizations never want to happen. A **business continuity plan** is a document that outlines the procedures to sustain business operations during and after a significant disruption. It is created alongside a disaster recovery plan to minimize the damage of a successful security attack. Here are four essential steps for business continuity plans:

- **Conduct a business impact analysis.** The business impact analysis step focuses on the possible effects a disruption of business functions can have on an organization.

- **Identify, document, and implement steps to recover critical business functions and processes.** This step helps the business continuity team create actionable steps toward responding to a security event.
- **Organize a business continuity team.** This step brings various members of the organization together to help execute the business continuity plan, if it is needed. The members of this team are typically from the cybersecurity, IT, HR, communications, and operations departments.
- **Conduct training for the business continuity team**. The team considers different risk scenarios and prepares for security threats during these training exercises.

Disaster recovery plan

A **disaster recovery plan** allows an organization's security team to outline the steps needed to minimize the impact of a security incident, such as a successful ransomware attack that has stopped the manufacturing team from retrieving certain data. It also helps the security team resolve the security threat. A disaster recovery plan is typically created alongside a business continuity plan. Steps to create a disaster recovery plan should include:

- Implementing recovery strategies to restore software
- Implementing recovery strategies to restore hardware functionality
- Identifying applications and data that might be impacted after a security incident has taken place

Juliana's story: Asset protection

Meet Juliana Soto, who recently completed an online cybersecurity certificate program and was hired as a cybersecurity analyst for Right-On-Time Payment Solutions, a fictional payment processing company allowing individuals to transfer money to friends and family. Right-On-Time also allows companies to accept payments from customers or organizations.

In this reading, you will begin a three-part journey that follows Juliana as she takes on new roles and responsibilities within the cybersecurity team of her new company.

Juliana decides that one of her first objectives is to gain a better understanding of the most important assets to the company by reviewing various company reading materials that will help her learn what is most valuable to them. On her first day, she is given reading materials to help her familiarize herself with the company. She learns that customers must create unique usernames and passwords and provide their full name or company name to sign up for the service as an individual. Business customers can also sign up for the service if they provide their employee identification number (EIN). Finally, customers must enter their bank account information or debit card number for payments to be accepted.

Juliana discovers that this company handles a lot of personally identifiable information (PII) from its customers. This kind of information is considered sensitive data. Unauthorized access to it can lead to significant damage to the organization's finances, its customers, and its reputation. Juliana realizes that the most important asset to this company is customer data.

After finishing the required onboarding materials, she decides to put together an information lifecycle strategy. She learned about this when completing her online cybersecurity certificate program.

Information lifecycle strategy

Juliana recalls the following steps of the information lifecycle:

- The first step in the information lifecycle is to identify the important assets to the company, including sensitive customer information such as PII, financial information, social security numbers, and EINs.

- The second step is to assess the security measures in place to protect the identified assets and review the company's information security policies. There are different components to this step, ranging from vulnerability scanning to reviewing processes and procedures that are already in place. Juliana is new to the company and might not be ready to conduct vulnerability scans.
- The third step of the information lifecycle is to protect the identified assets of the organization. Once again, this is only Juliana's first day on the job. She asks her supervisor if she can observe a more senior security analyst for a day. This will give her the opportunity to learn how the security team monitors the company's systems and network.
- The last step of the security lifecycle is to monitor the security processes that have been implemented to protect the organization's assets. She contacts her supervisor and gives them a detailed report of what she has learned on her first day. She requests to finish her day by monitoring a few of the systems that are in place. Her supervisor is impressed with her initiative and prepares Juliana to monitor the security systems. What a great first day for Juliana!

Module 2 - Escalate incidents

Escalate with a purpose

You previously learned about security incident escalation and the skills needed to help you escalate incidents. In this reading, you'll learn the importance of escalating security issues and the potential impact of failing to escalate an issue.

Incident escalation

Security incident escalation is the process of identifying a potential security incident. During this process, potential incidents are transferred to a more experienced department or team member. As a security analyst, you'll be expected to recognize potential issues, such as when an employee excessively enters the wrong credentials to their account, and report it to the appropriate person. When you join a new organization, you'll learn about the specific processes and procedures for escalating incidents.

Notification of breaches

Many countries have breach notification laws, so it's important to familiarize yourself with the laws applicable in the area your company is operating in. Breach notification laws require companies and government entities to notify individuals of security breaches involving personally identifiable information (PII). PII includes personal identification numbers (e.g., Social Security numbers, driver's license numbers, etc.), medical records, addresses, and other sensitive customer information. As an entry-level security analyst, you'll need to be aware of various security laws, especially because they are regularly updated.

Low-level security issues

Low-level security issues are security risks that do not result in the exposure of PII. These issues can include the following and other risks:

- An employee having one failed login attempt on their account
- An employee downloading unapproved software onto their work laptop

These issues are not significant security challenges, but they must be investigated further in case they need to be escalated. An employee typing in a password two to three times might not be of concern. But if that employee types in a password 15 times within 30 minutes, there might be an issue that needs to be escalated. What if the multiple failed login attempts were a malicious actor attempting to compromise an employee's account? What if an employee downloads an internet game or software on their work laptop that is infected with malware? You previously learned that malware is software designed to harm devices or networks. If malware is downloaded onto an organization's network, it can lead to financial loss and even loss of reputation with the organization's customers. While low-level security issues are not considered significant security threats, they should still be investigated to ensure they result in minimal impact to the organization.

The escalation process

Every company has different protocols and procedures, including unique escalation policies. These policies detail who should be notified when a security alert is received and who should be contacted if the first responder is not available. The policy will also determine how someone should specifically escalate an incident, whether it's via the IT desk, an incident management tool, or direct communication between security team members.

Recognize roles and responsibilities during escalation

You previously learned about various incident classification types and how those incidents can impact an organization.
This reading will discuss the roles of the various team members who are a part of the incident escalation process. Keep in mind that not all organizations are alike, and some roles and responsibilities may be identified using different terminology and definitions.

Data owners

A data owner is the person that decides who can access, edit, use, or destroy their information. Data owners have administrative control over specific information hardware or software and are accountable for the classification, protection, access, and use of company data. For example, consider a situation where an employee gains unauthorized access to software they do not need to use for work. This kind of security event would be escalated to the data owner of that software.

Data controllers

Data controllers determine the procedure and purpose for processing data. This role largely focuses on collecting the personal information of customers. The data controller determines how that data is used. The data controller also ensures that data is used, stored, and processed in accordance with relevant security and privacy regulations. If sensitive customer information was at risk, that event would be escalated to data controllers.

Data processors

Data processors report directly to the data controller and are responsible for processing the data on behalf of the data controller. The data processor is typically a vendor and is often tasked with installing security measures to help protect the data. Data processing issues are typically escalated to the individual who oversees the third-party organization responsible for data processing.

Data custodians

Data custodians assign and remove access to software or hardware. Custodians are responsible for implementing security controls for the data they are responsible for, granting and revoking access to that data, creating policies regarding how that data is stored and transmitted, advising on potential threats to that data, and monitoring the data. Data custodians are notified when data security controls need to be strengthened or have been compromised.

Data protection officers (DPOs)

Data protection officers are responsible for monitoring the internal compliance of an organization's data protection procedures. These individuals advise the security team on the obligations required by the organization's data protection standards and procedures. They also conduct assessments to determine whether or not the security measures in place are properly protecting the data as necessary. DPOs are notified when set standards or protocols have been violated.

Escalation timing

You previously learned about the potential impact even the smallest incident can have on an organization if the incident is not escalated properly. You also discovered just how important your role as an entry-level analyst will be to the effectiveness of an organization's escalation process. This reading will go into more detail about the role you'll play in protecting an organization's data and assets when it comes to escalating incidents.

Your decisions matter

Security is a fast-paced environment with bad actors constantly trying to compromise an organization's systems and data. This means security analysts must be prepared to make daily decisions to help keep a company's data and systems safe. Entry-level security analysts help the security team escalate potential security incidents to the right team members. A big part of your role as a security analyst will be making decisions about which security events to escalate before they become major security incidents.

Trust your instincts and ask questions

Confidence is an important attribute for a security analyst to have, especially when it comes to the escalation process. The security team will depend on you to be confident in your decision-making. You should be intentional about learning the organization's escalation policy. This will help you gain confidence in making the right decisions when it comes to escalating security events. But remember to ask questions when necessary. It shows that you're committed to constantly learning the right way to do your job.

All security events are not equal

An important part of escalation is recognizing which assets and data are the most important for your organization. You can determine this information by reading through your onboarding materials, asking your supervisor directly about which assets and data are most important, and reviewing your company's security policies. When you have that type of understanding, it allows you to recognize when one incident should be given a higher priority over others. You previously learned about the following incident classification types:

- **Malware infections:** Occur when malicious software designed to disrupt a system infiltrates an organization's computers or network
- **Unauthorized access:** Occurs when an individual gains digital or physical access to a system, data, or application without permission

- **Improper usage:** Occurs when an employee of an organization violates the organization's acceptable use policies

Identifying a specific incident type allows you to properly prioritize and quickly escalate those incidents. Remember, an incident which directly impacts assets that are essential to business operations should always take priority over incidents that do not directly impact business operations. For example, an incident where unauthorized access has been gained to a manufacturing application should take priority over an incident where malware has infected a legacy system that does not impact business operations. As you gain experience in the cybersecurity field, you will learn how to quickly assess the priority levels of incident types.

Quick escalation tips

A big part of your role in cybersecurity will be determining when to escalate a security event. Here are a few tips to help with this:

- Familiarize yourself with the escalation policy of the organization you work for.
- Follow the policy at all times.
- Ask questions.

Juliana's story: Attention to detail

This is the second reading in the scenario about Juliana Soto, a cybersecurity analyst who was recently hired by Right-On-Time Payment Solutions. In the reading about asset protection, Juliana identified important assets to her organization and came up with a plan for how to protect them. In this reading, you will review how Juliana used her company's escalation policy and her attention to detail to deal with security issues she encountered on the job.

Focus on the details

As she prepares to go into the office this morning, Juliana reflects on the previous day's accomplishments:

- Read through company information to learn about the most important assets she is tasked with protecting
- Learned that her company deals with PII data from customers
- Put together an information security lifecycle strategy for the organization's data
- Began monitoring security systems on her work laptop

It was an exciting first day full of new information for Juliana! She wonders what today will bring. Juliana is at her desk monitoring data logs and responding to emails. Suddenly, her system alerts her of suspicious log activity. It appears that an employee's account has been locked due to 10 failed login attempts. She finds this concerning because the escalation policy states that 10 failed login attempts should be escalated to the password protection team.

Juliana is excited about her first chance to escalate a security event. As she prepares to go through the escalation process, she is suddenly alerted to another event that has happened. She clicks on the alert and learns that an unknown source has attempted to compromise a system that stores bank account information for the company's customers. She views this as a major concern. She recalls the importance of sensitive financial information from her previous security training. She learned the previous day that her company stores a large amount of sensitive customer data. Hundreds of customers will be impacted if a system storing this kind of important data is compromised.

Juliana decides that the unknown source attempting to compromise the system that stores the bank information of customers is the more urgent of the two events and needs to be handled immediately. She references the company's escalation policy to find the best way to handle the escalation process for this type of incident.

Juliana carefully follows the process outlined in the escalation policy, making sure to be attentive to all of the details in the process. This allows her to notify the appropriate team members of what has happened. She completes all the steps outlined in the escalation policy for an event dealing with customer PII.

Next, she decides to escalate the lower-priority event. Once again, she follows the company guidelines to escalate that event.

Juliana's supervisor is impressed with her initiative and ability to follow the escalation guidelines. Juliana is off to a great start in her security career!

Module 3 - Communicate effectively to influence stakeholders

Who are stakeholders?

A **stakeholder** is defined as an individual or group that has an interest in any decision or activity of an organization. A big part of what you'll do as a security analyst is report your findings to various security stakeholders.

Levels of stakeholders

There are many levels of stakeholders within larger organizations. As an entry-level analyst, you might only communicate directly with a few of them. Although you might not communicate with all of the security stakeholders in an organization, it's important to have an understanding of who key stakeholders are:

- A cybersecurity risk manager is a professional responsible for leading efforts to identify, assess, and mitigate security risks within an organization.
- A Chief Executive Officer, also known as the CEO, is the highest ranking person in an organization. You are unlikely to communicate directly with this stakeholder as an entry-level analyst.
- A Chief Financial Officer, also known as the CFO, is another high-level stakeholder that you're unlikely to communicate with directly.
- A Chief Information Security Officer, also known as the CISO, is the highest level of security stakeholder. You are also unlikely to communicate directly with this stakeholder as an entry-level analyst.
- An operations manager oversees the day-to-day security operations. These individuals lead teams related to the development and implementation of security strategies that protect an organization from cyber threats.

CFOs and CISOs are focused on the big picture, like the potential financial burden of a security incident, whereas other roles like operations managers are more focused on the impact on day-to-day operations. Although you will rarely interact directly with high-level security stakeholders, it's still important to recognize their relevance.

Stakeholder communications for entry-level analysts

Two examples of security stakeholders with whom you might regularly communicate are operations managers and risk managers. When you report to these stakeholders, you'll need to clearly communicate the current security issue and its possible causes. The operations managers will then determine next steps and coordinate other team members to remediate or resolve the issue.

For example, you might report multiple failed login attempts by an employee to your operations manager. This stakeholder might contact the employee’s supervisor to ensure the occurrence is a genuine issue of entering the wrong password or determine if the account has been compromised. The stakeholder and supervisor might also need to discuss the consequences for day-to-day operations if genuine failed login attempts can lead to account lockouts that might impact business operations. As an entry-level security analyst, you might play a role in implementing preventative measures once next steps have been determined.

From one stakeholder to the next

Operations managers and risk managers are stakeholders who rely on entry-level analysts and other team members to keep them informed of security events in day-to-day operations. These stakeholders commonly report back to the CISOs and CFOs to give a broader narrative of the organization's overall security picture. Although you won't regularly communicate with high-level stakeholders, it's important to recognize that your efforts still reach the highest levels of security stakeholders in the organization. These other members of your team keep those top-level stakeholders informed on the security measures and protocols in place that are continuously helping to protect the organization.

Communicate effectively with stakeholders

You previously learned about security stakeholders and their significance in an organization. In this reading, you’ll learn the importance of clearly communicating to stakeholders to ensure they have a thorough understanding of the information you’re sharing and why it’s meaningful to the organization.

Get to the point

Security stakeholders have roles and responsibilities that are time sensitive and impact the business. It’s important that any communications they receive, and the actions they need to take, are clear. To get to the point in your communications, ask yourself:

- What do I want this person to know?
- Why is it important for them to know it?
- When do they need to take action?
- How do I explain the situation in a nontechnical manner?

Follow the protocols

When you first join a security team, you’ll want to learn about the different protocols and procedures in place for communicating with stakeholders and other members of the organization. It’s important to make sure you know what applications and forms of communications are acceptable before you begin communicating with stakeholders, such as in-person meetings, video-conferencing, emails, or company chat applications.

Communicate with impact

You previously learned about the different stakeholders within an organization and what specific areas they’re focused on. When you first begin your career in the cybersecurity field, you're more likely to interact with lower-level stakeholders, like operations managers or security risk managers, who are interested in the day-to-day operations, such as logging. Senior-level stakeholders might be more interested in the underlying risks, such as the potential financial burden of a security incident—as opposed to the details around logs.

When you communicate with an operations manager, make sure you address relevant information that relates to their daily responsibilities, such as anomalies in data logs that you are escalating. Concentrating on a manager's daily responsibilities will help you communicate the need-to-know information to that individual.

Communication methods

Your method of communication will vary, depending on the type of information you're sharing. Knowing which communication channels are appropriate for different scenarios is a great skill to help you communicate effectively with stakeholders. Here are a few ways you might choose to communicate:

- Instant messaging
- Emailing
- Video calling
- Phone calls
- Sharing a spreadsheet of data
- Sharing a slideshow presentation

If your message is straightforward, an instant message or phone call might be the route to take. If you have to describe a complex situation with multiple layers, an email or in-person meeting might be the better option. If you're providing a lot of data and numbers, sharing a graph might be the best solution. Each situation helps you determine the best means of communication.

Create visual dashboards for impactful cybersecurity communications

You previously learned about security stakeholders, the people responsible for protecting the data and systems of various departments of an organization. An entry-level analyst might communicate directly or indirectly with these individuals. If you do end up communicating with a stakeholder, it's important to use the right method of communication. This reading will further elaborate on the significance of using visual dashboards to communicate information to stakeholders. Dashboards can include charts, graphs, and even infographics. You'll learn more about when to use visual communication strategies in this reading.

Using visuals to communicate effectively

Security is about protecting a company from threats that can affect its reputation and finances. Oftentimes, responding to threats quickly and effectively depends on clear communications between the stakeholders who are involved.

In the cybersecurity field, the stakeholders you'll deal with will often be busy with other responsibilities. Showing them important information visually is a great way to gain their input and support to address security challenges that arise. Visuals help provide these decision-makers with actionable information that can help them identify potential risks to the organization's security posture.

Visual dashboards

A **visual dashboard** is a way of displaying various types of data quickly in one place. Visual dashboards are useful tools that can be used to communicate stories to stakeholders about security events—especially when they involve numbers and data.

Dashboards can be simple or complex depending on the information you're communicating. A simple dashboard might contain a single chart, while a complex one can include multiple detailed charts, graphs, and tables. Deciding which type to use will depend on the situation and story you are telling. However, attention to detail and accurately representing information is important anytime you're communicating data to stakeholders.

Pro tip: Programs like Google Sheets and Apache OpenOffice are tools that can be used to create visual dashboards.

When to use visual communication

Security is often a team effort. Everyone must work together to ensure an organization is properly protected from bad actors. Knowing how to communicate with your colleagues is a big part of the team-focused aspect.

Sometimes it's enough to send a simple email update. Other times you might want to include a document attachment that further elaborates on a specific topic. A simple phone call can also be valuable because it allows you to quickly communicate the necessary information without having to wait for a response to an email or message. Other times, the best way to communicate is through visuals.

For example, consider a situation where your supervisor has asked you to provide them with results from a recent internal audit of five different departments within the organization. The audit gathered data showing how many phishing emails each department clicked over the last five months. This is an ideal opportunity to tell this story using visualization tools. Instead of sending an email that simply describes what the findings are, a graph or chart will clearly illustrate those findings, making them easier for the stakeholder to understand quickly and easily.

Module 4 - Engage with the cybersecurity community

Juliana's story: Effective communication

Throughout this course, you've been following the story of Juliana Soto. Juliana was recently hired as a cybersecurity analyst by Right-On-Time Payment Solutions, a payment processing company that handles sensitive customer information. In the reading about attention to detail, Juliana had to deal with two different types of security incidents, and she used her company's escalation policy to properly escalate the two incidents. Now you will review how Juliana handled communication with stakeholders after escalating the incidents.

Communicating with stakeholders after an incident

Days after escalating the two incidents, Juliana's manager asks her to communicate information about the incidents to stakeholders.

Communicating about incident #1

One of the incidents dealt with an employee being locked out of their account due to multiple failed login attempts. Juliana's manager was recently asked to provide a report that reviews how many departments have experienced locked employee accounts due to failed login attempts over the last month. The security team shared data that details the number of locked employee accounts due to multiple failed login attempts from five different departments.

Juliana's manager will report the information to the senior executives of each of the five departments. The manager asks Juliana to display the data in a way that communicates the incident clearly to these stakeholders. For this task, Juliana decides to put together a visual dashboard to represent the data because the communication is primarily focused on numbers. Her dashboard will use charts and graphs to relay important information, like the number of employees who have been locked out of their accounts in the last month. Juliana's visual dashboard makes it easier for the high-level stakeholders to review incident #1 and determine a course of action.

Communicating about incident #2

Juliana’s manager has also been informed that the Chief Information Security Officer (CISO) wants more information about what took place during the second incident, which involved an attacker almost compromising a system that stores customers’ private data. This communication will include a more detailed report that establishes what processes and procedures worked well during attackers' attempts to compromise the system and what processes and procedures might need to be revised. Because this is a more detailed communication, Juliana decides to put together a detailed document with timelines that clearly explain what happened. The document also includes her thoughts on what the security team, data owners, and data processors could have done differently to protect the system in question. She shares the report with her manager so they can review it.

Strategies for engaging with the cybersecurity community

You have learned a lot about the security field, from the origins of security and its importance to organizations around the world to recognizing security incidents and communicating with stakeholders.

Security is a rapidly evolving industry, so it’s important to stay up-to-date on the latest news and trends. This reading will focus on how to stay engaged with the cybersecurity community after completing this program.

Security organizations and conferences

Attending security conferences and joining organizations gives you the opportunity to gain knowledge from seasoned professionals who are constantly seeking out new ways to improve on their security strategies and techniques.

Find the right organization

What security organization should you join? This question depends on your specific interest in security. Are you someone who wants to focus on reacting to security incidents or preventing them from happening? Are you interested in forensic security or data logging? Do you have aspirations of being a CISO one day? It’s important to have a clear understanding of what your interests are before you narrow down your search for a cybersecurity organization or conference.

Begin the search

Once you understand what your interests are, do a web search for organizations or conferences in your area. For example, you can type in “incident response cybersecurity conferences in my area.” This search will give you a list of cybersecurity conferences focused on incident response. If you’re interested in forensic security, you can type “forensic security organizations in my area” or a similar phrase into your web search engine. No matter what your interests are, you can do a web search online to find a cybersecurity organization or conference focused on that area.

Use social media

Social media is another great way to find cybersecurity organizations or conferences. LinkedIn®, for example, is a social media platform that connects business professionals with one another. You can use LinkedIn® to find security groups or organizations to join. In the LinkedIn® search bar, you can try search queries such as:

- "Incident response cybersecurity groups"
- "Organizations for cybersecurity analysts"

Be aware of social engineering

While social media is a good way to connect with other professionals in the security industry, it's also important to be mindful that hackers use social media to trick users into giving up private information. You've previously learned that social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. To protect yourself from social engineering when using social media to find resources, always remember not to click on unexpected links or attachments sent from unfamiliar users on social media.

Mailing lists for security

Another great way to stay connected with the security industry is to sign up for different cybersecurity mailing lists. These mailing lists send out information periodically on various security topics. The Cybersecurity & Infrastructure Security Agency (CISA) offers two cybersecurity mailing lists for you to join:

- A list focused on security threat information, best practices for cybersecurity, and analysis from CISA's domestic and international security partners
- A list providing weekly summaries of new vulnerabilities that might pose a risk to an organization's network

Connect with other cybersecurity professionals

You've learned the importance of staying engaged with the cybersecurity community after completing this certificate program. The security industry is always evolving, so it's important that security professionals continue to learn about the field.

This reading will focus on providing more tips to help you stay engaged with the security community and advance your career by engaging with the cybersecurity community.

LinkedIn® with CISOs

Earlier in the program, you learned about Chief Information Security Officers, also known as CISOs. It's their job to be up-to-date on every aspect of security, including all of the latest trends and news in the security world. With this in mind, it's a great idea to follow CISOs on LinkedIn® professional networking services. When you follow a CISO on social media, you'll have an opportunity to discover the kinds of information they share with their audience. That information might provide you with useful tips and relevant news. Staying informed about security news and trends can help progress your cybersecurity career because it helps sharpen your security mindset.

Finding other security professionals on LinkedIn®

Whether you'd like to connect with other entry-level analysts or more seasoned professionals, LinkedIn® is a great way to connect with others. When connecting with others, it's important to send a well-written message. This message can help the person understand your intentions. It also helps people determine that you’re not a scammer looking to exploit them. Here are a few tips to help you write your first message in a way that engages and interests the recipient:

- Use a conversational tone.
- Provide a clear reason for wanting to connect.
- Avoid spelling and grammatical errors.

Here is an example of an effective LinkedIn® message to send to a security professional:
“Hi, Tim. I recently completed the Google Cybersecurity Certificate program, and I’d like to connect with other security professionals. It seems like you have a lot of experience in the security industry that I can learn from. Let’s keep in touch!”
This example provides a clear reason for why you want to connect with this person and is presented in a conversational tone. You also did not give the impression that you are a scammer by asking the person to do something suspicious to connect with you, like downloading an unusual file attachment.

Module 5 - Find and apply for cybersecurity jobs