Negative threats, Risks, and vournerabilities

- Threats, risks, and vulnerabilities
- Herbert: Manage threats, risks, and vulnerabilities
- NIST’s Risk Management Framework
- Manage common threats, risks, and vulnerabilities
- Wrap-up

Threats, risks, and vulnerabilities

As an entry-level security analyst, one of your many roles will be to handle an organization's digital and physical assets.
As a reminder, an asset is an item perceived as having value to an organization.
During their lifespan, organizations acquire all types of assets, including physical office spaces, computers, customers' PII, intellectual property, such as patents or copyrighted data, and so much more.
Unfortunately, organizations operate in an environment that presents multiple security threats, risks, and vulnerabilities to their assets.
Let's review what threats, risks, and vulnerabilities are and discuss some common examples of each.

A threat is any circumstance or event that can negatively impact assets.
One example of a threat is a social engineering attack.
Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
Malicious links in email messages that look like they're from legitimate companies or people is one method of social engineering known as phishing.
As a reminder, phishing is a technique that is used to acquire sensitive data, such as user names, passwords, or banking information.

Risks are different from threats.
A risk is anything that can impact the confidentiality, integrity, or availability of an asset.
Think of a risk as the likelihood of a threat occurring.
An example of a risk to an organization might be the lack of backup protocols for making sure its stored information can be recovered in the event of an accident or security incident.
Organizations tend to rate risks at different levels: low, medium, and high, depending on possible threats and the value of an asset.

A low-risk asset is information that would not harm the organization's reputation or ongoing operations, and would not cause financial damage if compromised.
This includes public information such as website content, or published research data.

A medium-risk asset might include information that's not available to the public and may cause some damage to the organization's finances, reputation, or ongoing operations.
For example, the early release of a company's quarterly earnings could impact the value of their stock.

A high-risk asset is any information protected by regulations or laws,
which if compromised, would have a severe negative impact on
an organization's finances, ongoing operations, or reputation.
This could include leaked assets with SPII, PII,
or intellectual property.

Now, let's discuss vulnerabilities.
A vulnerability is a weakness that can be exploited by a threat.
And it's worth noting that both a vulnerability and
threat must be present for there to be a risk.
Examples of vulnerabilities include: an outdated firewall, software, or
application; weak passwords; or unprotected confidential data.
People can also be considered a vulnerability.
People's actions can significantly affect an organization's internal network.
Whether it's a client, external vendor, or employee,
maintaining security must be a united effort.

So entry-level analysts need to educate and
empower people to be more security conscious.
For example, educating people on how to identify a phishing email is a great starting point.
Using access cards to grant employee access to physical spaces while
restricting outside visitors is another good security measure.
Organizations must continually improve their efforts when it comes to
identifying and mitigating vulnerabilities to minimize threats and risks.
Entry-level analysts can support this goal by encouraging employees to
report suspicious activity and actively monitoring and
documenting employees' access to critical assets.

Now that you're familiar with some of the threats, risks, and
vulnerabilities analysts frequently encounter,
coming up, we'll discuss how they impact business operations.

Herbert: Manage threats, risks, and vulnerabilities

My name is Herbert and I am a Security Engineer at Google.
I think I've always been interested in security,
in high school our school gave us these huge Dell laptops.
There wasn't a whole lot of security within those computers.
So, many of my friends would have cracked versions of like video games like Halo,
that's really where I learned how to start manipulating computers to kind of do what I want.
I guess [LAUGH] my day to day consists of analyzing security risks and
providing solutions to those risks.
A typical task for
cybersecurity analysts would usually be something like exceptions requests.
Analyzing if someone needs to have special access to a device or document
based on the role that the person has or the project that they're working on.
One of the more common threats that we come across is misconfigurations or
requesting access for something that you don't really need.
For example, I recently had a case where a vendor we
were working with had changed their OAuth scope requests.
And basically that means that they were requesting more permissions to use Google services than they had before in the past.
We weren't sure really how to go about that because that wasn't
a situation we've come across before.
So it's still ongoing, but
we're working with partner teams to kind of develop a solution for that.
I think another thing that we've seen is outdated systems,
machines that need to be patched.
That sounds like an IT issue, but it's also definitely a cybersecurity issue.
Having outdated machines, not having proper device management policies,
working with a team or many teams is a huge part of the job.
In order to get really anything done, you need to communicate with not just the team that you're a part of, but with other teams.
Ten years ago I was working at a pizza joint and ten years later,
here I am, at Google as a Security Engineer.
If I told my 16 year old self that I would be here,
I wouldn't have believed myself, but it is possible.

NIST’s Risk Management Framework

As you might remember from earlier in the program, the National Institute of Standards and Technology, NIST, provides many frameworks that are used by security professionals to manage risks, threats, and vulnerabilities.

In this video, we're going to focus on NIST's Risk Management Framework or RMF. As an entry-level analyst, you may not engage in all of these steps, but it's important to be familiar with this framework. Having a solid foundational understanding of how to mitigate and manage risks can set yourself apart from other candidates as you begin your job search in the field of security.

There are seven steps in the RMF: prepare, categorize, select, implement, assess, authorize, and monitor.

Let's start with Step one, prepare. Prepare refers to activities that are necessary to manage security and privacy risks before a breach occurs. As an entry-level analyst, you'll likely use this step to monitor for risks and identify controls that can be used to reduce those risks.

Step two is categorize, which is used to develop risk management processes and tasks. Security professionals then use those processes and develop tasks by thinking about how the confidentiality, integrity, and availability of systems and information can be impacted by risk. As an entry-level analyst, you'll need to be able to understand how to follow the processes established by your organization to reduce risks to critical assets, such as private customer information.

Step three is select. Select means to choose, customize, and capture documentation of the controls that protect an organization. An example of the select step would be keeping a playbook up-to-date or helping to manage other documentation that allows you and your team to address issues more efficiently.

Step four is to implement security and privacy plans for the organization. Having good plans in place is essential for minimizing the impact of ongoing security risks. For example, if you notice a pattern of employees constantly needing password resets, implementing a change to password requirements may help solve this issue.

Step five is assess. Assess means to determine if established controls are implemented correctly. An organization always wants to operate as efficiently as possible. So it's essential to take the time to analyze whether the implemented protocols, procedures, and controls that are in place are meeting organizational needs. During this step, analysts identify potential weaknesses and determine whether the organization's tools, procedures, controls, and protocols should be changed to better manage potential risks.

Step six is authorize. Authorize means being accountable for the security and privacy risks that may exist in an organization. As an analyst, the authorization step could involve generating reports, developing plans of action, and establishing project milestones that are aligned to your organization's security goals.

Step seven is monitor. Monitor means to be aware of how systems are operating. Assessing and maintaining technical operations are tasks that analysts complete daily. Part of maintaining a low level of risk for an organization is knowing how the current systems support the organization's security goals. If the systems in place don't meet those goals, changes may be needed.

Although it may not be your job to establish these procedures, you will need to make sure they're working as intended so that risks to the organization itself, and the people it serves, are minimized.

Manage common threats, risks, and vulnerabilities

Previously, you learned that security involves protecting organizations and people from threats, risks, and vulnerabilities. Understanding the current threat landscapes gives organizations the ability to create policies and processes designed to help prevent and mitigate these types of security issues. In this reading, you will further explore how to manage risk and some common threat actor tactics and techniques, so you are better prepared to protect organizations and the people they serve when you enter the cybersecurity field.

Risk management

A primary goal of organizations is to protect assets. An **asset** is an item perceived as having value to an organization. Assets can be digital or physical. Examples of digital assets include the personal information of employees, clients, or vendors, such as:

- Social Security Numbers (SSNs), or unique national identification numbers assigned to individuals
- Dates of birth
- Bank account numbers
- Mailing addresses

Examples of physical assets include:

- Payment kiosks
- Servers
- Desktop computers
- Office spaces

Some common strategies used to manage risks include:

- **Acceptance**: Accepting a risk to avoid disrupting business continuity
- **Avoidance**: Creating a plan to avoid the risk altogether
- **Transference**: Transferring risk to a third party to manage
- **Mitigation**: Lessening the impact of a known risk

Additionally, organizations implement risk management processes based on widely accepted frameworks to help protect digital and physical assets from various threats, risks, and vulnerabilities. Examples of frameworks commonly used in the cybersecurity industry include the National Institute of Standards and Technology Risk Management Framework (NIST RMF) and

Health Information Trust Alliance (HITRUST).

Following are some common types of threats, risks, and vulnerabilities you'll help organizations manage as a security professional.

Today's most common threats, risks, and vulnerabilities

Threats

A **threat** is any circumstance or event that can negatively impact assets. As an entry-level security analyst, your job is to help defend the organization's assets from inside and outside threats. Therefore, understanding common types of threats is important to an analyst's daily work. As a reminder, common threats include:

- **Insider threats:** Staff members or vendors abuse their authorized access to obtain data that may harm an organization.
- **Advanced persistent threats (APTs):** A threat actor maintains unauthorized access to a system for an extended period of time.

Risks

A **risk** is anything that can impact the confidentiality, integrity, or availability of an asset. A basic formula for determining the level of risk is that risk equals the likelihood of a threat. One way to think about this is that a risk is being late to work and threats are traffic, an accident, a flat tire, etc.

There are different factors that can affect the likelihood of a risk to an organization's assets, including:

- **External risk:** Anything outside the organization that has the potential to harm organizational assets, such as threat actors attempting to gain access to private information
- **Internal risk:** A current or former employee, vendor, or trusted partner who poses a security risk
- **Legacy systems:** Old systems that might not be accounted for or updated, but can still impact assets, such as workstations or old mainframe systems. For example, an organization might have an old vending machine that takes credit card payments or a workstation that is still connected to the legacy accounting system.
- **Multiparty risk:** Outsourcing work to third-party vendors can give them access to intellectual property, such as trade secrets, software designs, and inventions.

- **Software compliance/licensing:** Software that is not updated or in compliance, or patches that are not installed in a timely manner

There are many resources, such as the NIST, that provide lists of cybersecurity risks. Additionally, the Open Web Application Security Project (OWASP) publishes a standard awareness document about the top 10 most critical security risks to web applications, which is updated regularly.

Note: The OWASP's common attack types list contains three new risks for the years 2017 to 2021: insecure design, software and data integrity failures, and server-side request forgery. This update emphasizes the fact that security is a constantly evolving field. It also demonstrates the importance of staying up to date on current threat actor tactics and techniques, so you can be better prepared to manage these types of risks.

Lists that compare the top 10 most common attack types between 2017 and 2021

Vulnerabilities

A **vulnerability** is a weakness that can be exploited by a threat. Therefore, organizations need to regularly inspect for vulnerabilities within their systems. Some vulnerabilities include:

- **ProxyLogon:** A pre-authenticated vulnerability that affects the Microsoft Exchange server. This means a threat actor can complete a user authentication process to deploy malicious code from a remote location.
- **ZeroLogon:** A vulnerability in Microsoft's Netlogon authentication protocol. An authentication protocol is a way to verify a person's identity. Netlogon is a service that ensures a user's identity before allowing access to a website's location.
- **Log4Shell:** Allows attackers to run Java code on someone else's computer or leak sensitive information. It does this by enabling a remote attacker to take control of devices connected to the internet and run malicious code.
- **PetitPotam:** Affects Windows New Technology Local Area Network (LAN) Manager (NTLM). It is a theft technique that allows a LAN-based attacker to initiate an authentication request.
- **Security logging and monitoring failures:** Insufficient logging and monitoring capabilities that result in attackers exploiting vulnerabilities without the organization knowing it
- **Server-side request forgery:** Allows attackers to manipulate a server-side application into accessing and updating backend resources. It can also allow threat actors to steal data.

As an entry-level security analyst, you might work in vulnerability management, which is monitoring a system to identify and mitigate vulnerabilities. Although patches and updates may exist, if they are not applied, intrusions can still occur. For this reason, constant monitoring is important. The sooner an organization identifies a vulnerability and addresses it by patching it or updating their systems, the sooner it can be mitigated, reducing the organization's exposure to the

vulnerability.

To learn more about the vulnerabilities explained in this section of the reading, as well as other vulnerabilities, explore the NIST National Vulnerability Database and CISA Known Exploited Vulnerabilities Catalog.

Key takeaways

In this reading, you learned about some risk management strategies and frameworks that can be used to develop organization-wide policies and processes to mitigate threats, risks, and vulnerabilities. You also learned about some of today's most common threats, risks, and vulnerabilities to business operations. Understanding these concepts can better prepare you to not only protect against, but also mitigate, the types of security-related issues that can harm organizations and people alike.

Resources for more information

To learn more, click the linked terms in this reading. Also, consider exploring the following sites:

- OWASP Top Ten
- NIST RMF

Wrap-up

You've now completed the first section of this course! Let's review what we've discussed so far.

We started out by exploring the focus of CISSP's eight security domains. Then, we discussed threats, risks, and vulnerabilities, and how they can impact organizations. This included a close examination of ransomware and an introduction to the three layers of the web.

Finally, we focused on seven steps of the NIST Risk Management Framework, also called the RMF.

You did a fantastic job adding new knowledge to your security analyst toolkit. In upcoming videos, we'll go into more detail about some common tools used by entry-level security analysts. Then, you'll have an opportunity to analyze data generated by those tools to identify risks, threats, or vulnerabilities. You'll also have a chance to use a playbook to respond to incidents. That's all for now. Keep up the great work!