**Communicating with Stakeholders: Your Role**

* Stakeholders receive **sensitive information**—be cautious about **what and who** you communicate with.
* Different stakeholders need updates on **different issues**, so tailor your communication accordingly.
* Communications should be:
  + **Clear**
  + **Concise**
  + **Focused** on purpose
  + Free of unnecessary technical jargon
* Remember, stakeholders are often **very busy**; make your messages easy to understand without guessing.
* **Ask your manager or supervisor** about stakeholder preferences and priorities to ensure relevant info sharing.
* Use your **security mindset** by asking questions about key assets and tools, for example:
  + “What data is most important to protect daily?”
  + “Which security tools are most effective?”
* Your communication helps stakeholders stay **informed** and perform their roles better.
* You play a vital role in delivering **critical, relevant information** to the right people.

**Creating Clear and Precise Security Communications**

* Effective security communication is like telling a story with a:
  + **Beginning** (the issue)
  + **Middle** (its impact)
  + **End** (possible resolution)
* The story explains the security challenge, its organizational impact, and potential solutions.
* Use relevant **data** such as reports or issue lists to support your message.
* Example scenario:
  + You detect potential malicious code execution in system logs.
  + Communicate this clearly to your supervisor.
  + Reference the organization’s **incident response playbook** to show adherence to procedures.
  + Suggest possible solutions even if you’re not the final decision-maker.
* Communication formats include:
  + Emails
  + Documents
  + Visual representations (graphs, charts, dashboards)
  + Incident management or ticketing systems
* Visual tools help stakeholders better understand complex security information.
* Mastering the ability to tell a clear security story helps stakeholders make informed decisions and makes their jobs easier.

**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.

**Key takeaways**

Stakeholders are busy people who have very specific interests within the organization. Therefore, it’s important to only communicate information that is specific to their interests and impacts their role in the company.

Be mindful of the kind of information you’re communicating because that will help determine what method of communication you should use.