

The purpose and impact of stakeholders

You previously learned about incident escalation and the various security incident classification types. You also learned about the impact these incidents can have on an organization's business operations.

This reading will explore the individuals who have a significant interest in those business operations: 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.

Key takeaways

Stakeholders play a major role in ensuring the security of an organization. Entry-level analysts should have a foundational understanding of the different levels of security stakeholders within an organization. Entry-level analysts will not communicate with every security stakeholder in a company, but there are certain stakeholders that the analyst will need to provide updates to. Those updates will eventually be reported up to the more senior-level stakeholders, such as the CISO and the CFO.

Revision #1

Created 9 January 2024 15:33:04 by naruzkurai

Updated 9 January 2024 15:33:34 by naruzkurai