Business continuity considerations

Previously, you learned about how security teams develop incident response plans to help ensure that there is a prepared and consistent process to quickly respond to security incidents. In this reading, you'll explore the importance that business continuity planning has in recovering from incidents.

Business continuity planning

Security teams must be prepared to minimize the impact that security incidents can have on their normal business operations. When an incident occurs, organizations might experience significant disruptions to the functionality of their systems and services. Prolonged disruption to systems and services can have serious effects, causing legal, financial, and reputational damages. Organizations can use business continuity planning so that they can remain operational during any major disruptions.

Similar to an incident response plan, a **business continuity plan (BCP)** is a document that outlines the procedures to sustain business operations during and after a significant disruption. A BCP helps organizations ensure that critical business functions can resume or can be quickly restored when an incident occurs.

Entry level security analysts aren't typically responsible for the development and testing of a BCP. However, it's important that you understand how BCPs provide organizations with a structured way to respond and recover from security incidents.

Note: Business continuity plans are not the same as *disaster recovery plans.* Disaster recovery plans are used to recover information systems in response to a major disaster. These disasters can range from hardware failure to the destruction of facilities from a natural disaster, like a flood.

Consider the impacts of ransomware to business continuity

Impacts of a security incident such as ransomware can be devastating for business operations. Ransomware attacks targeting critical infrastructure such as healthcare can have the potential to cause significant disruption. Depending on the severity of a ransomware attack, the accessibility, availability, and delivery of essential healthcare services can be impacted. For example, ransomware can encrypt data, resulting in disabled access to medical records, which prevents healthcare providers from accessing patient records. At a larger scale, security incidents that target the assets, systems, and networks of critical infrastructure can also undermine national security, economic security, and the health and safety of the public. For this reason, BCPs help to minimize interruptions to operations so that essential services can be accessed.

Recovery strategies

When an outage occurs due to a security incident, organizations must have some sort of a functional recovery plan set to resolve the issue and get systems fully operational. BCPs can include strategies for recovery that focus on returning to normal operations. Site resilience is one example of a recovery strategy.

Site resilience

Resilience is the ability to prepare for, respond to, and recover from disruptions. Organizations can design their systems to be resilient so that they can continue delivering services despite facing disruptions. An example is site resilience, which is used to ensure the availability of networks, data centers, or other infrastructure when a disruption happens. There are three types of recovery sites used for site resilience:

- **Hot sites**: A fully operational facility that is a duplicate of an organization's primary environment. Hot sites can be activated immediately when an organization's primary site experiences failure or disruption.
- **Warm sites**: A facility that contains a fully updated and configured version of the hot site. Unlike hot sites, warm sites are not fully operational and available for immediate use but can quickly be made operational when a failure or disruption occurs.
- **Cold sites**: A backup facility equipped with some of the necessary infrastructure required to operate an organization's site. When a disruption or failure occurs, cold sites might not be ready for immediate use and might need additional work to be operational.

Key takeaways

Security incidents have the potential to seriously disrupt business operations. Having the right plans in place is essential so that organizations can continue to function. Business continuity plans help organizations understand the impact that serious security incidents can have on their operations and work to mitigate these impacts so that regular operations can resume.

Mark as completed

Like **Dislike** **Report an issue**