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 three 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

Key takeaways

Disaster recovery and business continuity plans are important for an organization's security posture. It's essential that the security team has plans in place to keep the organization's business operations moving forward in case a security incident does occur.

Mark as completed