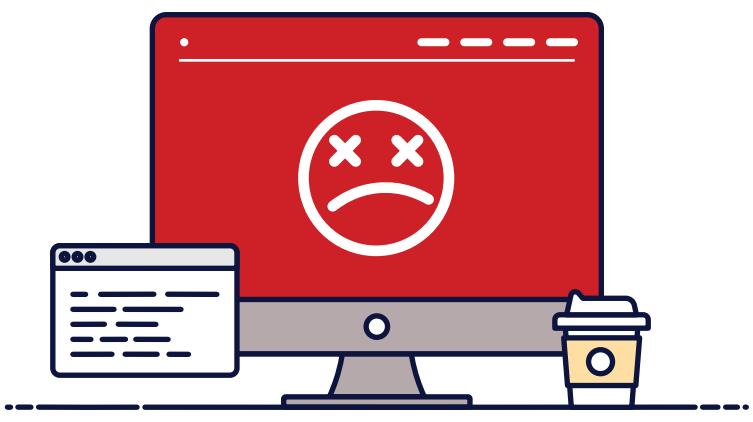
IS YOUR BUSINESS PREPARED FOR A CYBER INCIDENT?



You probably have a savings account set aside for a rainy day, coverage for your home in case your basement floods and insurance for your car to cover accident repairs. What would you do if your business gets targeted by a cyberattack? You'll need a plan for that, too.

While the best approach to prevent a cyber incident is with proactive cybersecurity technologies and team awareness training, it isn't always enough. You'll need a strategy in place to address incidents as they occur. This strategy is called **incident response.**

CYBER INCIDENT RESPONSE TERMINOLOGY

CYBER INCIDENT

A cyber incident can refer to any event that causes you to lose data or your network and tech systems to go down. This can include events like phishing attacks, malware/ransomware infections or denial-of-service attacks.

INCIDENT RESPONSE

A swift and effective incident response helps your business analyze, detect, defend against and respond to a cyber incident and recover quickly.

INCIDENT HANDLING

The incident handling process is a set of procedures for you to follow as soon as an incident is detected. This process includes planning and taking action before, during and after an incident.

INCIDENT MANAGEMENT

Incident management is a combination of both incident response and incident handling. This is important because it identifies, diagnoses and resolves incidents while taking steps to prevent future incidents.

INCIDENT RESPONSE PLAN

A well-documented incident response plan helps employees detect and respond to security incidents effectively. It should help the affected technology recover successfully and minimize data loss or service outages.

WHAT DOES AN INCIDENT RESPONSE LOOK LIKE?

IDENTIFY

There are many security risks that you need to be aware of to develop an effective incident response plan. This includes dangers to your technology systems, data, operations and more. By understanding these risks, you can be better prepared to respond to incidents and minimize the impact of security breaches.

PROTECT

Creating and implementing appropriate safeguards is crucial to protecting your business. Security measures to guard against threats and steps to ensure the continuity of essential services in the event of an incident are examples of safeguards.

DETECT

Your organization needs processes and tools to detect irregularities such as unusual activity on your network or someone trying to access sensitive data. This helps you limit the damage and get your systems back up and running faster by detecting incidents quickly.

RESPOND

It is vital to have a plan in place to respond to detected cyber incidents. This plan should include strategies for containing, investigating and resolving breaches.

RECOVER

Following an incident, you need a plan to restore normal business operations as quickly as possible to minimize disruption.

If you're concerned about how to handle IT incidents, teaming up with an IT service provider can go a long way toward putting your mind at ease.

Contact us today for a no-obligation consultation and we can help you get started.

Z-JAK Technologies

www.zjak.net
info@zjak.net
(502) 200-1169