CYBERSECURITY INCIDENT

RESPONSE PLAN

KALARA®

How can a cyberattack be prevented from becoming a complete breach? Prepare ahead of time. Organisations frequently realise that they could have avoided a significant amount of expense, suffering, and disruption if they had an effective incident response plan in place after a breach.

Cybersecurity incident response plan

An efficient plan for responding to an incident consists of ten main steps.

1. Establish key stakeholders
2. Classify critical assets
3. Conduct tabletop exercises
4. Implement protection tools
5. Ensure you have complete visibility
6. Execute access control
7. Invest in analysis tools
8. Determine response actions
9. Perform awareness training
10. Appoint a managed security service

1. Establish key stakeholders

The security team isn't the only one who needs to properly prepare for an eventuality. Almost every department in the organisation will be affected by an incident, particularly if the incident develops into a comprehensive breach. Before you can effectively coordinate a response, you need to figure out who should be involved. Senior management, security, IT, legal, and public relations are frequently represented in this.

It's important to know in advance who should sit at the table and participate in the planning activities of your organisation. To ensure a prompt response, a means of communication must also be established. Take into consideration the possibility of an incident affecting your usual means of communication, such as email.

2. Classify critical assets

The business must first identify its most important assets before determining the scope and impact of an attack. In addition to assisting you in devising a defence strategy, mapping out your most important assets will make it much simpler to ascertain an attack's scope and impact. The incident response team will also be able to focus on the most important assets during an attack if these are identified in advance, minimising disruption to the business.

3. Conduct tabletop exercises

Like many other fields, incident response is one in which practice makes perfect. Practice exercises ensure a more tightly coordinated and effective response in the event of a real breach, despite the difficulty of fully replicating the intense pressure your team will experience. Technical tabletop exercises, which are frequently conducted as part of a red team drill, are important, but so are more general exercises that include the various business stakeholders that were previously identified.

The organisation's responses to a variety of possible incident response scenarios should be tested through tabletop exercises. Stakeholders outside the immediate technical team might also be involved in each scenario. Even if an attack was successfully defended, your company should decide in advance who needs to be informed.

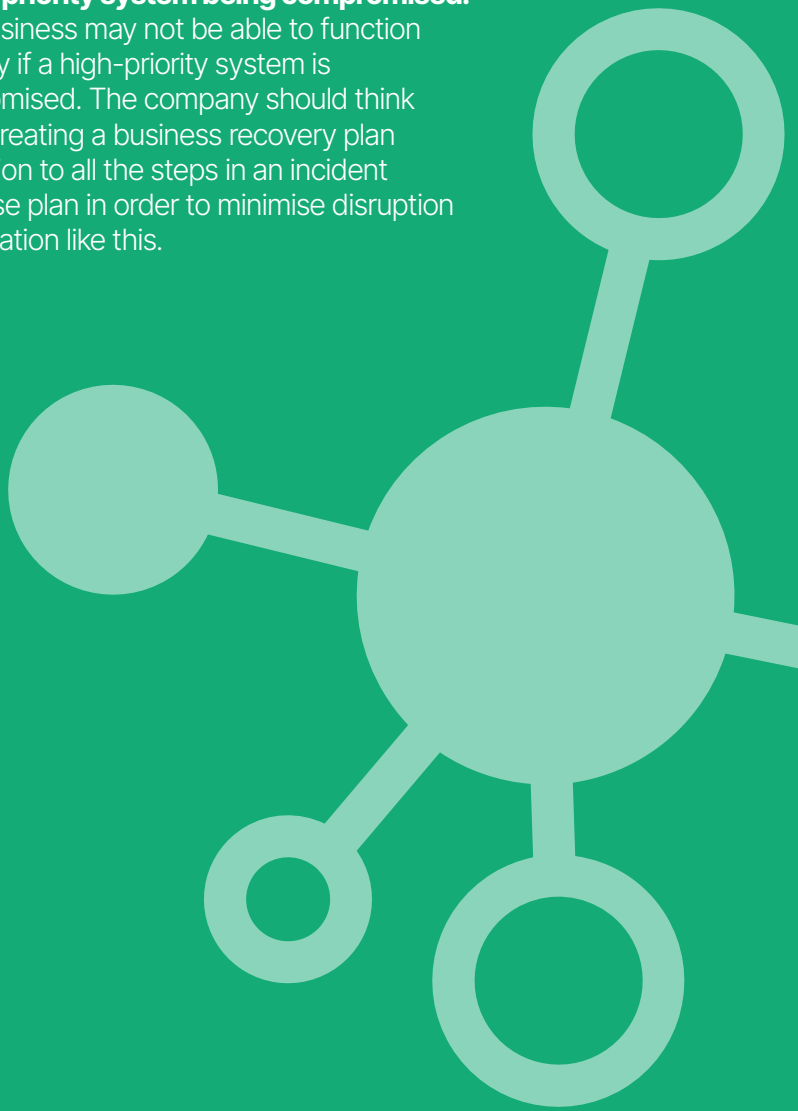
Typical scenarios for handling an incident include: Within your network, an active adversary was discovered: The response team must determine how an attacker entered your environment, what they used, what they were targeting, and whether they have established diligence in these scenarios. The best way to stop the attack will be determined with the help of this information.

While it might seem obvious to remove the adversary from the environment right away, some security teams prefer to observe the attacker to gather important information about what they're trying to accomplish and how they're doing it.

A successful data breach: Your team should be able to determine what was exfiltrated and how in the event that a successful data breach is discovered. This will then inform the appropriate response, including whether customers need to be contacted.

Attack by ransomware that succeeded: Your team should follow a plan to quickly recover from losses if critical data and systems are encrypted. A procedure for restoring systems from backups should be included in this. The team needs to determine whether the adversary's access has been blocked in order to guarantee that the attack won't reoccur as soon as you return online. In addition, the organisation as a whole should ascertain whether and how much it would be prepared to pay a ransom in extreme circumstances.

A high-priority system being compromised: Your business may not be able to function normally if a high-priority system is compromised. The company should think about creating a business recovery plan in addition to all the steps in an incident response plan in order to minimise disruption in a situation like this.



4. Implement protection tools

Preventing an incident from occurring in the first place is the best course of action. Check to see that the organisation has the right endpoint, network, server, cloud, mobile, and email protection.

5. Ensure you have complete visibility

The company won't be able to respond appropriately during an attack if it doesn't have adequate visibility into what is going on. IT and security teams need to be able to identify adversary entry points and points of persistence before an attack takes place in order to comprehend its scope and impact.

For proper visibility, log data must be collected, with an emphasis on endpoint and network data. It is essential to have historical data going back days, weeks, or even months in order to investigate as many attacks take days or weeks to discover. In addition, make sure that such data is backed up so that it can be accessed in the event of an active incident.

6. Execute access control

Access control flaws can be exploited by attackers to breach the organisation's defences and gain access. Make certain that the appropriate controls for establishing access control are in place on a regular basis.

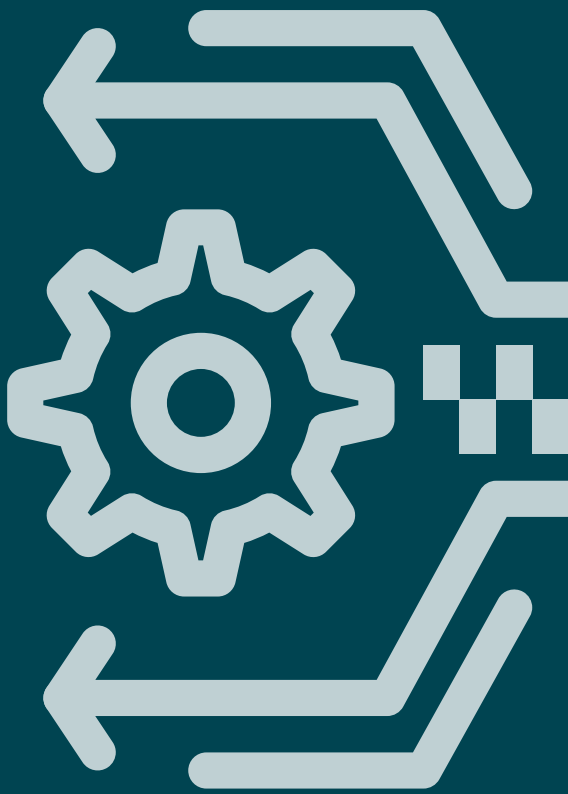
Changing default passwords, implementing multi-factor authentication, restricting admin privileges to as few accounts as possible (in accordance with the Principle of Least Privilege), and reducing the number of access points you need to monitor are all examples of this.

7. Invest in analysis tools

The organisation should invest in tools that provide the necessary context during an investigation in addition to ensuring that you have the necessary visibility.

Endpoint detection and response (EDR) and extended detection and response (XDR) are two of the most widely used tools for incident response. These tools let you search across your environment to find indicators of compromise (IOCs) and indicators of attack (IOA). Analysts can use EDR tools to identify which assets have been hacked, which in turn helps them figure out the impact and scope of an attack. During the investigation, more context is available the more data is collected from the endpoints and beyond. Your team will be able to determine not only what the attackers targeted, but also how they entered the environment and whether they still have the ability to access it again with greater visibility.

Advanced security teams may also implement a security orchestration, automation, and response (SOAR) solution that facilitates response workflows in addition to EDR tools.



KALARA®

8. Determine response actions

An attack can only be detected in part. IT and security teams must be able to carry out a wide range of corrective actions to deter and eliminate an attacker in order to effectively respond to an attack. Among the responses are, but are not limited to Isolating affected hosts.

- Blocking malicious files, processes, and programs
- Blocking control and malicious website activity
- Freezing compromised accounts and cutting off access to attackers
- Cleaning up adversary artefacts and tools
- Closing entry points and areas of persistence leveraged by attackers (internal and third-party)
- Adjusting configurations (threat policies, enabling endpoint security and EDR on unprotected devices, adjusting exclusions, etc.)
- Restoring impacted assets via offline backups

9. Perform awareness training

Education programs, such as phishing awareness, help reduce your risk level and the number of alerts your team must respond to, but no training program will ever be 100% effective against a determined adversary. Using tools to simulate phishing attacks gives your staff a safe way to experience (and possibly fall victim to) a phish, enrols those who fail training, and identify risky user groups for whom additional training may be required.

10. Appoint a managed security service

Numerous organisations lack the capacity to deal with incidents on their own. Experienced security personnel are needed to respond quickly and effectively. Consider working with a managed detection and response (MDR) provider to ensure that you can respond appropriately.

Summary

When a cybersecurity incident occurs, immediate action is required. The impact of an attack on your organisation will be significantly reduced if you have a well-thought-out, well-prepared response plan that can be immediately implemented by all key parties.

t: 01293265777

e: hello@kalara.co.uk