Cybersecurity Planning Guide

How to create a plan for responding to a cybersecurity attack

With news of new threats and more sophisticated attack methods breaking every day, businesses need to strengthen their cyber security practices now more than ever. We have long advocated for our clients to prepare for such an event and work closely with our cyber security partner, ESET, to help ensure they are as well prepared as they can be.

So, what is the best way to avoid having a cyberattack turn into a full breach? Prepare in advance of course. Putting in place an Incident Response Plan will help you to respond to an incident quickly to help minimise losses, mitigate vulnerabilities, restore services more swiftly and reduce the risks of future potential attacks.

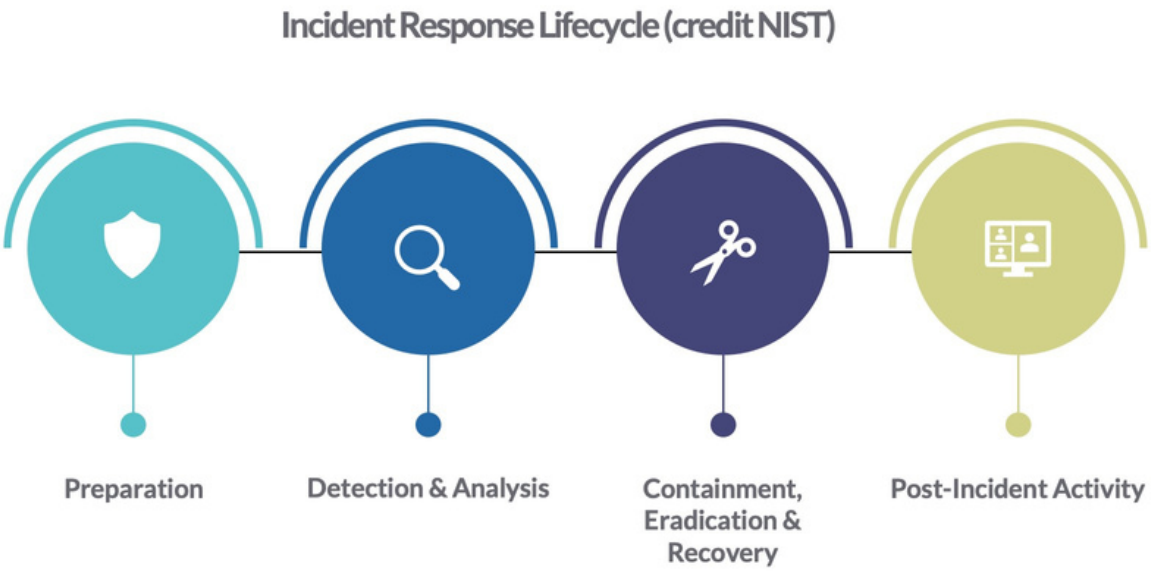
Not every adverse event requires a full-blown response and indeed, automated tools often manage these well enough. However, for those times when more sinister patterns and intent are at play, such as multiple single attacks or an inexplicable system failure occurs, then how are you going to manage this and limit potential damage?

Cybersecurity Planning Guide

The Four Phase Incident Response

This guide follows best advice from the National Institute of Standards and Technology (NIST) and ESET, to help you to develop a well-thought-out incident response plan, so you can confidently manage attacks with the support of your in-house IT team or partner.

NIST publication, the Computer Security Incident Handling Guide (SP 800-61), details four phases of incident response and each are covered in more detail below.



1. Preparation

This phase is all about ensuring you have all the appropriate security controls in place before any incident happens. This means your ICT infrastructure must be built and maintained with security a top priority.

This includes keeping servers, operating systems and applications up to date, suitably configured and fortified with malware protection. Your network perimeter should also be properly secured via firewalls and VPNs.

One factor that is often forgotten about is your employees. Often viewed as the weakest link in cyber security, it's crucial to ensure they are trained appropriately and regularly to prevent security breaches.

Once the infrastructure is in place then careful monitoring and management is vital to identify, collect and analyse any adverse events. There are various options available for this, but your IT support team or partner will be able to advise on the most appropriate for your specific requirements.

Creating an incident response team

This may seem like overkill, especially in a small business, but having a team of key stakeholders in place that can respond rapidly to incidents will enable your business to manage an adverse event more effectively and recover as soon as possible.

An incident is not the sole responsibility of your IT or security team as they will likely impact almost every department of you organisation. So, your team should include individuals that have the knowledge of how your infrastructure is built and what normal operation looks like (so you will need to involve your IT support team or partner), and those that are able to make timely decisions and make the necessary resources available to effectively manage the issue (probably senior management).

All individuals will have a role to play, whether that's a practical one, for example shutting down servers, or assessing the implications of doing so from a financial, legal and customer service perspective.

2. Detection & Analysis

Without proper visibility into what is happening during an attack, then you will struggle to respond appropriately. This phase is all about having the right resources in place to enable the business to interpret the data captured by the monitoring tools and to understand exactly what has happened.

This will invariably require someone with strong cyber security knowledge, from your IT support team or potentially an external resource, who may recreate sequences of events leading to the incident to identify the root cause. While the motivation is to move to phase 3 as quickly as possible, incident responders may conduct further root cause analysis to uncover additional data that warrants further investigation.

3. Containment, Eradication & Recovery

In this third stage, the incident response team decides on how to stop the further spread of detected threats. Any containment action decisions need to consider the potential for further damage while also preserving evidence.

Various decisions will need to be made at this stage, including whether a server should be shut down, an endpoint isolated, or certain services stopped. This could result in isolating compromised systems, segmenting parts of the network, or putting affected machines in a secure environment for testing.

Once contained, any discovered malware needs to be deleted from compromised systems. User accounts may need to be disabled, closed or reset. Vulnerabilities should be patched, systems and files should be restored from clean backups, passwords should be changed, firewall rules should be tightened, and so the list goes on.

A full return to normal business operations can take months depending on the incident. In the short term, increased or more finely tuned logging and monitoring should be established so that IT admins can prevent the same incident from happening again. The longer term might see more overarching infrastructure changes to help transform the network into a more secure one.

4. Post-Incident Activity

The incident response team should document and provide an event reconstruction and timeline. This helps to understand the root cause of the incident and what can be done to prevent a repeat or similar incident.

This is also the time for all teams to review the effectiveness of the processes and procedures used, identify gaps in communication and collaboration, and look for opportunities to introduce efficiencies to the current incident response plan.

Finally, the response team needs to decide on the retention policy for evidence collected during the incident. So, don't just the wipe the hard drives without first consulting your legal department. Most organisations archive incident records for two years to comply with regulations.

When a cybersecurity incident strikes, time is of priority. Having a well prepared plan will dramatically reduce the impact of an attack on your organisation.

However, we realise that for many organisations this will undoubtably be new territory, so we recommend involving your IT support team or partner as early in the process as possible.