SIDN For confidence online

How to produce a Cyber Incident Response Plan

A step-by-step guide for SMEs

'Incident response' is the term given to the process of dealing with a data leak or cyber-attack, including efforts to mitigate the consequences. All with the ultimate goal of minimising both the financial and reputational damage and the time it takes to get your business back on its feet. The five phases of a good incident response are described in another article. The Cyber Incident Response Plan is a document describing the various types of cyber-incident and the associated response processes. It serves as a game plan for the action needed in the event of a hack or data leak.

Tip! *You can, of course, draw up a plan single-handed if you like. But it often makes sense to get together people from the different disciplines within your organisation for a brainstorming session. After all, two (or more!) heads are better than one. Working together usually results in a better plan and promotes awareness within the organisation.*

Step 1: Assemble an incident response team

If you're ever hit by a cyber-attack, it's likely that numerous things will need doing at once. So divide responsibility across a team.

- Whose job is it to coordinate the response?
- Who will analyse the attack?
- Who's responsible for communication with customers and other stakeholders?

Step 2: Perform a risk analysis

A risk analysis provides a starting point for effective incident detection monitoring and risk reduction. In order to build up a picture of potential risks, ask yourself the following questions:

- What incidents have occurred in the past?
- What threats exist?
- What systems do we have, and which of them are vulnerable?
- Which threats are most likely to materialise?
- Are our staff aware of the risks?

For each threat that you identify, decide how likely it is to materialise; grade its probability as low, medium or high. Then decide how serious it would be if it did materialise; grade its seriousness as low, medium or high. You've then got a list of the main risks that you face.

Tip! *Business proprietors can be a little blind to internal issues. So it can help to ask an outside security expert to take a look at your systems.*

Step 3: Draw up an action plan

Once you know what the main risks facing your business are, you can guard against them. For each risk, produce a scenario:

- What kind of incident might occur?
- What would need to be done if an incident did occur?
- Which (external) players would be involved or would you need to get involved?
- Who would need to be informed?
- Who would be responsible for doing what?

Answering those questions in advance will help you act decisively if an incident does actually occur.

SIDN For confidence online

Step 4: Set up an alarm mechanism

If anyone in your business realises than an incident is likely or already in progress, they need to raise the alarm straight away.

- Who do they tell, and how?
- What if the incident occurs outside working hours?

Step 5: Tell staff about the plan

Make sure that everyone knows about the response plan, and keep reminding them. No matter how good your plan is, it's of little use if people don't know it exists or where to find it.

And don't forget about newcomers: make sure they're told about the plan when they start.

Step 6: Hold regular drills

Give your staff regular training so they know what to do if there's an incident. Incident drills work like fire drills. If you've been in a situation before – for real or in a drill – you do what you need to do better and more quickly.

Hold a drill once a quarter, focusing on one of the incident types identified in your risk analysis. When you're done, evaluate the drill. What went well and what could be improved? That way, you increase the likelihood that your staff flag up incidents promptly and are ready to act.

Step 7: Learn from actual incidents

You might think you've covered all the bases in your Cyber Incident Response Plan. But, in practice, there will always be things you could have predicted and things you could have done better, differently or faster.

Learn from your experiences, so you can adapt your plan and be better prepared for future incidents.

Step 8: Make sure the plan is accessible

Think carefully about where you keep your plan. If it's only on SharePoint, say, you won't be able to get to it if your network is paralysed by ransomware. So it makes sense to have copies in several places.

- Where should we keep our Incident Response Plan?
- Should the whole plan be available to everyone, or do most staff only need the alarm procedure?

The five phases of good incident response

Your plan is nearly complete, but good incident response depends on successfully completing five phases.
We recommend including them in your plan. There's more about the five phases on sidn.nl.

This checklist was compiled by SIDN. For more about how we can help with business cybersecurity, visit sidn.nl.