What to include in your incident response plan

Criminals act fast and encourage panic to achieve their objectives. An incident response plan will keep you organised and in control during a pressure situation.

Timely decision making is essential during a cyber attack. Similarly to fire drills, you should prepare for the worst-case scenario; review and practice the plan to identify gaps and be confident that it will be fit for purpose.

Here is a brief summary of what to include in your incident response plan:

Prioritise

Assess the type and severity of the attack; where does it classify on a "critical" to "low risk" register? Find out the top threats to your business and envisage how the attack will play out from identifying the attack to recovery. The threat will be less daunting if you understand what you are up against and sound preparation potentially reduces the impact.

Contact List

Identify key contacts for during and after the incident e.g. tech support, PR, web developer, insurance, ICO, Action Fraud. Then create an incident response team and assign roles; these contacts need to be prominent in the plan so everyone knows exactly who to notify and, importantly, when.

Make a back-up plan with alternative contact details – an attack might make email and/or phones unusable. DO NOT make a single individual critical to the plan – sods law she will be on leave when the attack comes!

Who to notify

Set the levels for when to escalate the incident. Know at what point you will inform senior management, ICO, etc and anyone impacted (such as customers, staff, and supply chain). Remember, you have 72 hours to report a data breach to the ICO and recognising the severity of threat will determine who to update and when.

Know your assets

Knowing in advance where important information and tools are stored (such as logs, asset register, map of the network) will greatly reduce your response time.

Legal obligations

Predetermine when you would consider collecting evidence and how best to do so e.g. notes, reports, observations, data capture. Some scenarios require you to document and report the incident to authoritative bodies; you may want to pursue legal action.

Considerations

Ask yourself the following questions: Can your team respond 24/7/365? How would you communicate efficiently if the usual platforms are unavailable? Which parts of the business are you willing to close down to contain an attack?

Have your playbook ready and be prepared to justify those decisions. There is no "one plan fits all" scenario but being aware of your options in advance will help you and your team to make informed decisions under pressure.

Communication

To avert unauthorised leaks your staff need to be advised of the incident and their responsibilities. It is vital that the whole business understands when and why action is to be taken, remember to summarise these actions in your plan.

The incident response process

1. **Analyse** Recognise what you are up against to plan your approach effectively, with the help of your incident response plan. Continue to examine the attack, you may need to r e-evaluate your tactics.
2. **Contain/Mitigate** When safe to do so and after careful analysis, launch measures that will reduce the impact of the threat, technically (such as isolating systems) and non-technically (such as media communications).
3. **Remediate/Eradicate** Remove the threat and examine its success. Once certain it no longer poses a problem, only then should you start the recovery phase. You may have to repeat other steps of the process before full remediation is achieved.
4. **Recover** At this stage you have confirmed the threat has gone and clean systems can be installed. Clean data backups can be recovered if needed, for business to resume as usual.
5. **Review** Following an incident, review lessons learned and document improvements in your incident response plan. Be aware of any secondary attacks, while you recover and you move forward.

For detailed incident response processes, visit the NCSC website:
https://www.ncsc.gov.uk/collection/incident-management

www.policedsc.com

POLICE DIGITAL SECURITY CENTRE