PlanB Consulting Downloads & Resources

Cyber Incident Response

“Thankfully, we now live in a world where it is accepted that data breaches happen and organisations are more comfortable disclosing that they have been victim to an attack.

However, with this welcome move away from victim blaming, organisations are now being judged more on how well they manage a breach.”

Brian Honan in Computer Weekly

What is a Cyber Incident?

The NCSC defines a cyber incident as unauthorised access (or attempted access) to an organisation's IT system/s. These may be malicious attacks such as denial of service attacks, malware infection, ransomware or more commonly phishing attacks.

An accidental action by an employee could also cause a security incident for example when a member of staff clicks on a phishing link within an email or downloading a seemingly legitimate piece of software as part of day to day work which contains a virus or malicious software.

How to respond when it happens to you

You may have spent a lot of time and money ensuring that your organisation will never suffer from a security breach, but if we accept that no system is 100% secure, the question becomes not **how protected** you are, but **how prepared** you are.

It is good practice to have a Cyber Incident Response Plan in place that sets out the steps your organisation should take to detect, respond and recover from cyber-attacks. Your plan does not have to be complex but it should be clear on the roles and responsibilities of key individuals who can take action. This should not sit in isolation and should be woven into the wider resilience, business and service continuity / disaster recovery planning.

What is a Cyber Playbook?

A playbook is typically associated with responding to a cyber incident and gives the actions, procedures and communications associated with responding to a certain incident. As per its name, it is derived from American Football. Plays are selected depending on the position on the field, strengths and weaknesses of the opposition and the stage of the game.

Two Different Sorts of Playbooks

There are two different types of playbooks which can be written to respond to cyber incidents. They are decision playbooks and response playbooks:

1. Decision Playbooks

In some incident responses, the way of resolving the incident may not be obvious and there may be a number of options which needed to be considered on the day of the incident and which one to take very much depends on the circumstances of the incident.

Typical examples of the decision could be:

- Do you switch to your alternative data centre or do you wait until the main comes up?
- Do you pay a cyber ransom?
- When do you need to inform those on your databases that their information has possibly been hacked?
- If you have denial of access attack do you disconnect your system from the internet?

In all of these examples, there is no obvious response and it will very much depend on the circumstances and will be a judgment call on the day. Often this judgement call might need to be made without the full facts being available and the consequences of whatever decision may be substantial.

Decision playbook contents

So, what might we want to record against each of the scenarios in our playbook, using the ‘whether we switch to the alternative data centre’ as an example?

1. What is the scenario the ‘play’ covers?
2. Options available?
3. What circumstance is there a clear decision?
4. What are the issues to be taken into account on making the decision?
5. How long does it take to implement the decision?
6. Who can make the decision?
7. What needs to be done to implement the decision, and who needs to do it?
8. What is the downside of operating the alternative?
9. What subsequent actions need to be taken and how will the recovery be carried out?

2. Response Playbooks

The second type of playbook is for a specific type of incident. Incidents don't always fit the plan, but some of the detailed planning is worth carrying out. These sort of cyber incident playbooks should be written for are the basic attacks including ransomware, DDoS attacks and data loss (this might want to be segregated into the different types of data the organisation hold). It is only worth writing these playbooks for larger incidents which would have a reputational impact, and for smaller incidents an IT response plan is sufficient.

Response playbook contents

These are the headings this type of playbook should have:

1. **Type** of incident – DDoS etc.

2. Likely means of **detection** – include the main ways the incident could be detected.

3. Likely **impacts** – which part of the organisation might be affected? E.g. ransomware could stop all company systems, but data loss will have no impact on actual systems.

4. **IT plans** in place for dealing with it and their strategy for recovery – crossreference the relevant IT plans.

5. **Who** needs to be informed of the incident, internally and externally? I think this is a key part so that you can quickly identify all those who might be affected. These should be segregated, so don't just include staff, as there could be contractors, temporary staff, those off sick, maternity/paternity leave, staff that have left and retirees. I also think there should be information on how to contact

your staff, as well as a plan on how to get in contact if the IT systems are down.

6. What **regulatory and statutory** notifications are required, including time frames and what information is needed? For example, reporting to regulators, Information Commissioners Office and the stock market.

7. How will the incident be **managed** and are there any requirements for specialists joining the incident team? Which team will manage the incident, and do you need specialists, such as external public relations help, plus legal and compliance people on the team?

8. What **third party** support is required? This could include forensic IT specialists.
9. **Risks, decisions and issues** to consider – as many as you can think of.

10. Guidance on **communications** and lines to take – this could be debated and exercised so that there is a structure in place already.

11. Relevant **business continuity plans** and recovery strategies – are there business continuity plans and manual workarounds which can help the response?

12. What actions can be taken to **support** those affected, and what support are you going to give the victims of the incident?

13. What **matrices** should be used and monitored to check the effect on the organisation? How do you tell if your response plans are being successful?

14. **Priorities** and predetermined objectives for this type of incident – can you write them now?

15. **Other** – under this heading, when choosing an example, I wrote ‘what data we hold’, so if this playbook was for a breach of the staff database, we know what data we hold on staff.

Cyber incidents by their nature are difficult to manage, especially at the beginning of the incident. If your headquarters burn down, the incident and the consequences are obvious, but if there is a cyber breach then there is nothing to see, so it can take a while to understand the true impact of the incident.

As with all business continuity, the more you plan, exercise and think about your response, the more you realise what you can do now, which will help your response on the day. The old army adage comes to mind “**train hard fight easy**”

Our Cyber Incident Response Services

PlanB Consulting supports businesses through their cyber responses across the globe. We offer a range of support including:

- **Cyber Gap Analysis**
  We assess your current readiness and equip your organisation to effectively respond to cyber incidents and manage cyber risk.

- **Cyber Exercises**
  We offer a wide range of cyber attack response exercises for organisations to explore and practice their incident management plans.

- **Cyber Briefings for Senior Managers**
  We are here to help your organisation be prepared to respond to cyber incidents and manage your cyber risk.

- **Writing Cyber Playbooks**
  We can help you create the Playbook for your Cyber Incident Response.

- **Training Courses**
  We offer NCSC Certified Cyber Incident Management Training via a 2 day non-technical course, aimed at preparing organisations to manage their cyber response at the strategic/crisis management level.

About PlanB Consulting

PlanB Consulting is a specialist business continuity consultancy, passionate in delivering long-term quality results for organisations in the private, non-profit and public sectors. As a specialist consultancy their competencies include full life cycle business continuity development, training and running exercises. The company is located in Houston near Glasgow and delivers services worldwide, but predominantly in the UK and Europe.

The company prides itself in keeping up with the latest business continuity tools, techniques and standards as well as writing business continuity content for blogs, journals, TV and radio. All staff within PlanB Consulting are passionate about their work and this enthusiasm is evident in the quality of work and their attitude on site.

Contact Us

PlanB Consulting
10, Business First
Burnbrae Road
Linwood
PA1 2FB

Tel 01505 22 88 98

Email info@planbconsulting.com