Best Practices for **Developing a Cyber Security Playbook**

What is a Cyber Security Playbook?

The majority of organisations plan for fires, floods, and other incident that impact business resilience and careful planning for a cyber security incident shouldn't be any different. The purpose of a Cyber Security Playbook,or Security Playbook, is to provide all members of an organisation with a clear understanding of their roles and responsibilities regarding cyber security – before, during and after a security incident.

A Security Playbook also defines the Crisis Communications Team (CCT) and establishes the contact liaison between the board and the rest of the organisation.

Once the team is defined and aware of their position, key action steps as a result of a cyber security incident also need to be put in place. These will include:

- Incident detection; notification, analysis and forensics
- Response actions; containment, remediation and restoration
- Communication; understand the lessons learned and manage media relations

There is no one-size fits all approach to Security Playbooks. Before defining the strategy right for your organisation, you should first have a clear understanding of what data is most important to protect.

Top tips: Before an incident

Crisis Communications Team (CCT)

The CCT needs to be put in place prior to an incident occurring. Various levels of personnel and departments need to be involved to ensure company-wide understanding and participation. The team should include:

- **CEO/CTO:** They are in-charge of dispersing the message throughout the organisation and communicating with the board
- **IT department:** Most likely to have the technical expertise, members of the IT department definitely need to be involved, however, it cannot be solely their responsibility
- **Media/PR:** Necessary to deal with the potential media coverage and disseminate the message agreed by the organisation
- **Legal counsel:** To provide legal insight into the impact and ensure the response is appropriate to meet compliance or regulatory requirements
- **Others:** The CEO/CTO must decide if other team members or departments need to be included in the CCT

Incident response plan

Following the establishment of the CCT, an incident response plan needs to be implemented, including a step by step guide of key actions to be taken in the wake of an incident. Investing in a response plan and employee training is a worthwhile investment, which helps to improve your organisation's Cyber Security Maturity. Practice drills and exercises are key, so that when an incident occurs, everyone is aware of the role they play and the impact can be minimised. Such exercises include; security awareness training – to educate employees on best practices, including those that have not had much to do with cyber security previously, social media and journalist simulations – how to handle the media and convey a collective message is a crucial element of crisis mitigation, and red-team exercises – this is a vigorous attempt to gain access to your organisation's systems, in order to define any weaknesses.

Nowadays, many people obtain news through social media. Ensuring that there is a clear, outlined social media strategy in the event of a breach is essential to keeping control of the situation. If tweets, comments or questions are coming in from the outside, the media relations team need to understand if, or how, they should respond.

When these weaknesses have been discovered, recovery plans need to be drawn up so everyone knows the necessary actions.

Top tips: During an incident

React fast

As soon as an incident occurs, the incident response plan needs to be put into play. The goal is to handle the incident in a way that limits both damage and impact, both financially and to the reputation of the organisation. The CCT need to be communicating with the entire organisation, top-level down, so everyone is aware of what they need to be doing. The lessons and best practices learned from the drills and mitigation tactics from red team exercises need to be implemented.

Gather data on the incident as it occurs, this will help exercises and planning for incidents in the future. Hindsight is a wonderful thing, but after the incident it is often too late to gather enough information to have a comprehensive view. Building out data on the breach as it occurs not only aids learning, but also helps speed up investigation and determining the cause.

The quicker and more effectively your reaction, the better the likelihood you have of reducing the impact and cost to the organisation.

Agree messaging

In this day and age, it is difficult to keep news under wraps. Often news of a breach or incident will be disseminated by third parties; this is why having a clear plan and process is crucial.

Working with the media relations and legal teams, the board needs to decide the messaging around the incident. This needs to include how much information and which bits of information regarding the incident will be disclosed. This should be the only message that is communicated on behalf of the organisation. No facts should be communicated until they have been verified.

Nowadays, with the growing prevalence of social media, organisations also need to be aware of communication channels. As part of the CCT, members of the media relations team need to be assigned with controlling the social media output; what's coming in as well as going out.

Communication

Clear and constant communication amongst the CCT needs to be upheld throughout the remediation efforts. As soon as communication lines drop, people can lose track of what they need to be doing – and this is where mistakes are made.

After an incident

As the remediation element of the incident response reaches its final stages, damage control needs to begin. There will undoubtedly be consequences as a result of what's happened, whether the impact is financial or reputational, this needs to be planned for and addressed in the right way for each business.

Once you've survived an incident, it's time to review how successful the incident response strategy was. Weaknesses in the equipment, systems and procedures need to be addressed to determine where improvements need to be made. Use what has happened as a lesson and learn from mistakes. Determine key areas of investment and look at where you can improve your Cyber Security Maturity levels.

If the incident has affected customers or, more specifically, their data, the board needs to work with the legal team to decide how this issue will be dealt with. The legal team needs to be included in this decision, as depending on the industry, there may be legislative requirements that need to be met.

Lastly, remain vigilant. Another incident, whatever the type, is going to occur. The most important thing is to ensure your organisation is as prepared as possible to handle it.

To find out how CNS Group can help your organisation to develop and implement a Cyber Security Playbook, or Incident Response Plan, click **here.**