Incident Response Plan Checklist

Creating an Incident Response Plan for your business is crucial and it is important that you are prepared in the event of one. We have put together a checklist to ensure you are taking the correct measures in developing your Incident Response plan.

Before an incident

- **Look to reduce risk of incident occurring**

Before a cyber security incident occurs, it is important to look at all the aspects of your organisation to see how you can reduce the risk of an incident occurring. This could be by reviewing infrastructure to minimize internet facing devices or segregating key systems such as online purchasing systems from the office environment. This is important to identify the risks and keep loss of revenue to a minimal.

- **Establish tools and controls**

Establishing tools and controls before an incident means that you will have the correct network detection software or the correct procedures for reviewing logs on servers, this is to flag unusual behaviour from a network. This is the act of creating the ability to detect an incident which you can respond to in a time efficient manner.

- **Develop containment plan**

As part of the incident response plan it is important to develop a containment plan in order to be able to keep effects of the breach to a minimal and effectively resolve the situation without affecting other networks or servers. It is important to add this to your response plan to establish how you will shut down the affected network or take the server offline to stop it from propagating.

- **Communication**

Deciding how and what you are going to communicate during a cyber security incident is essential. You will need to know what you are going to tell your staff and any clients who will be affected in the event of a cyber-attack, such as if your clients or customers data was to be breached. You will also have to decide whether you are going to communicate with the press and if so, what details you share, and which member of staff is going to communicate it.

- **Disaster recovery plan**

A Disaster Recovery Plan (DRP) is a documented process or set of procedures to recover and protect a business' IT infrastructure in the event of a disaster. Disaster Recovery is an integral part of overall risk management for organizations small and large alike. In the event of a disaster, it is vital to have a set plan in place to know how to recover any disrupted IT systems and data to mitigate loss and disruption.

During an incident

- **Invoking containment plan, communication and DRP**

Once an incident has occurred you will need to follow through with your containment plan, communication plan and the disaster recovery plan which you initially set out to follow. It is important to stick to your procedures and the preparation that you have done to ensure business operations are restored as quickly as possible.

After an incident

- **Determine information accessed and lost through attack**

After the cyber security incident has occurred, it is important to determine the impact of the breach, the systems which were affected or compromised. It is also important to check the system logs to perform forensics, after doing this you should contact the ICO and they will help you establish a plan to contact any affected third parties.

- **Communication**

Statements will need to be released to customers or clients in event of a data breach to inform them of what has happened and if any of their information has been breached. If you are giving statements to the press, follow your communication plan and ensure your staff are informed of what to say and what information to keep private.

- **Lessons learned from the incident**

After the incident you will need to determine the nature of the attack, what you did well and how you could improve in event of another one. For example, staff may require more training on how to deal with the situation or if your plan hasn't been effective you may need to address any gaps for the future.

CS Risk Management offer workshops ranging from 1-2 days for businesses looking to implement or learn more about cyber security incident responses. This helps your employees to learn the procedure and ensure that anyone who is going to have an impact on responding to the incident knows what they must do and keep negative impacts and losses to a minimum.

We also provide 1-day workshops to deliver security-related training which can consist of; IT staff training, Communication Plans, Recovery Plans, Maximum Tolerable Period of Disruption and more.

If you would like to find out more about this, then please contact us today.