Incident response: Five key steps organisations need to take following a security breach

These days data breaches are an all too common occurrence. Barely a week goes by without another high-profile attack taking place. With increasing legislation and regulatory requirements coming into play; these announcements are likely to become more prominent.

There's much advice given about how to reduce the risk of an attack and the different preventative measures that organisations can put in place. However, with new technologies and routes of entry for attackers, preventive measures alone are not enough. In order to ensure all bases are covered, organisations need to be prepared with a solid security incident response plan. When an incident occurs, it will ensure everyone knows exactly what to do to minimise the impact to their organisation.

Why do some organisations not have incident response plans in place?

Many organisations lack incident response plans for the same reason most people don't get travel insurance before going on holiday, or check their tyre pressure before driving long distances. Most people don't think about these things until it's too late. Developing and implementing a security incident response plan can be time consuming and often costly – two things most organisations do not have. Without a response plan, incidents can escalate quickly and the impact can be severe. An incident response plan gives organisations a much better chance of isolating and controlling an incident in a timely and cost effective manner.

A recent Incident Response Survey uncovered concerns by IT professionals about their organisation's security incident response plans. Twenty-six percent of respondents were not confident in their organisation's security response plan. Despite this continued lack of confidence, respondents understood the significant impact of a breach upon their organisations with reputational damage topping the list (56 percent), loss of system availability (13 percent), compliance issues (11 percent), loss of IP (nine percent), remediation costs (nine percent) and other (two percent).

When asked why they thought an organisation would not have a response plan in place, lack of awareness within organisations came out on top with 38 percent of respondents highlighting this as an issue. This was followed by a lack of resources (23 percent), lack of skills or expertise (18 percent), lack of budget (12 percent), other (nine percent) and lack of time (five percent). Coming from IT professionals, the perceived lack of awareness when it comes to incident response plans is worrying.

Five key steps to take following a security breach

So, the worst has happened and your organisation has suffered a security breach. What are the first things you need to do to ensure that your risk is minimised?

1. Triage

   Don't panic – it may be a natural reaction, but from our experience, it doesn't solve anything. Avoid the temptation to simply pull the plug or turn the machines off. Directly after a breach, things often seem worse than they are. Your main goal should be business continuity. To do this, it's important to establish the nature and extent of the incident. Is it something that has been seen before, such as a common ant-virus incident? If so what steps need to be taken to control the impact of the incident?

   It's crucial to closely manage any communication about the security breach to customers and beyond. Many security breaches are broken by news outlets watching social media feeds. Make sure you have a dedicated team in place for crisis communications and keep track of all customer interactions. This will help you better manage public relations following the incident.

2. Data analysis

   Carefully analysing the data involved in the incident is crucial to understanding what actually happened. It may sound simple but over the years, we have seen too many cases that are misdiagnosed early on, resulting in incorrect remedial actions. For example, diagnosing a DDOS attack when a completely different failure has occurred or prepping for a data corruption incident when it's actually ransomware. Understand what happened and how, if this is something that you don't have the time or resources to manage in your organisation, call in cyber security experts to help you figure out what happened. By assigning an expert to handle the incident, you can be sure the responsibility of incident management and coordination is taken care of, so that you can focus on getting your organisation back to its normal state of operation.

3. Communication

One of the biggest issues we see with incident response is a lack of internal communication – from board level down. Depending on the type of incident, it may be that communication with the rest of the organisation and external bodies such as third-party agencies, customers and regulatory authorities is necessary. If that is the case, it's important to ensure communication only occurs through the pre-planned and established channels.

Communication cannot just take place after the incident. It needs to be an on-going process throughout the organisation. Regardless of their job function, when a security incident occurs, everyone needs to be fully trained and aware of their role and responsibilities. Putting security incident playbooks in place for each department can be one way to keep staff aware of what they are and are not allowed to do in the wake of a breach. As outlined in step one, taking charge of your communication channels is crucial. You should be the one to decide when and how news of the breach is disseminated to various parties. This will help minimise the impact of the incident and fan any flames.

4. Resolve and recover

Assuming the incident handler and the technical team assigned to the incident has control, you should be on the way to resolving the issue and heading towards recovery. The road to recovery may involve rolling back disaster recovery (DR) applications, beginning to restore data from backups or simply closing the incident. Whatever the situation, the incident will not be properly resolved until all recovery actions are complete.

5. Lessons learned

Following an incident, organisations can be quick to fall back into routine. It's important that you learn from every security incident to minimise the risk of it taking place in the future. Ask yourself; what can we implement to better protect ourselves? If this happens again, have we done enough to minimise the risk and disruption? Does everyone know their role and are they aware of the role they play in keeping the organisation secure?

Top tips for developing an incident response plan

One of the first things we introduce when discussing incident response plans with customers is Security Incident Playbooks. This works by identifying key risk areas, determining what working state you are operating in and ensuring everyone is aware of the appropriate actions:

- First of all, an organisation must establish a scoring methodology for identifying its key threat actors and threat vectors – who is likely to be targeting your organisation and through what means?
- This methodology can then be used to decide the organisation's current working state; whether its normal, high, elevated or severe
- The right Security Playbooks should then be deployed. These are ways of working and actions developed for each department. This means everyone, no matter what their job role, has a part to play in managing the organisation's security and knows how to respond when an incident occurs
- Security Playbooks need to be well documented and easy for everyone in the organisation to access. Through a Wiki or Intranet – they also need to be kept up-to-date and amended to address new risks. That way, when a breach occurs, everyone is aware of their required actions
- Regular and up-to-date staff training is also important. Although cyber security cannot be seen physically, its importance should not be underestimated. In the constantly evolving threat landscape, everyone needs to be kept well-informed of new dangers.

Simple steps, like ensuring all data and devices are properly encrypted and keeping access to classified information limited can also minimise the risk of a security incident. Most people think a security incident has to be a major breach, but more often than not they are the result of something much more basic.

The benefits of an incident response plan and when to call in the experts

The benefits of a security incident response plan are clear. As well as having much better preventative methods in place to manage risks, when an incident does occur there is a more rapid response. This quick action is key to minimising the impact of any incident.

Developing and implementing incident response plans can take considerable time, money and skills – which organisations often don't have. That's why a lot of organisations choose to outsource incident response to specialists who are equipped to deal with these situations. Incident response teams are experienced to understand the different types of threat actors and vectors, and how this varies by company size and industry.

Security Playbooks and staff training require constant re-development and needs to be provided on a continuous basis. As well as having the expertise required to develop in-depth knowledge materials, incident response experts also have the resources and up to date expertise necessary to maintain these.

Most organisations turn to their IT departments to provide this level of cyber security care, but it's rarely the case that they have the man-power or knowledge to provide the required level of service. By outsourcing incident response, organisations can be sure they have a dedicated team on hand, who know what to look out for and are ready to respond.

*To find out more about CNS Group's incident response service, **click here.***

Our business is securing your data

As a government accredited company, we help UK organisations of all sizes build cyber security capabilities and maintain compliance through practical consulting and Managed Security Services. For more information on how our Managed Security Services can help protect your business, click here or contact us now on:

info@cnsgroup.co.uk

020 7592 8800

@CNS_Security

www.cnsgroup.co.uk

© Convergent Network Solutions Ltd