



Why all businesses need an incident response plan

There needs to be a change in attitude towards the threat of cyber attacks.



Almost every day we seem to hear about businesses suffering from security breaches. Just recently, news emerged that up to 26 million NHS patients might be at risk of having their records compromised due to an unsecure IT system that thousands of GPs use. GP leaders claimed that the situation could have “potentially huge implications” if a data breach were to occur, and the story has led to complaints from many patients.

This is just one of many cyber security-related stories that have made the headlines in recent weeks, and while there’s been no confirmation of a breach or the seizure of confidential patient records, it does nothing to help the NHS’ reputation — quite the opposite, in fact. What’s more, it proves that absolutely any business can find itself embroiled in a serious cyber-security situation, no matter what size or sector it operates in.

The statistics on cyber attacks are astounding. According to the National Crime Agency, there were 2,500,000 attacks in the UK alone last year — with some saying that the number should actually be much higher — and GCHQ is set to spend more than £420,000 on hiring new cyber security experts to deal with cases such as these. While it’s hoped that this investment will reduce the impact of cyber attacks, hackers are continually evolving and learning how to stay one step ahead of the authorities, meaning that no business should consider itself truly safe.

With this in mind, there needs to be a change in attitude towards the threat of cyber attacks. While businesses used to think they could get away with taking a more laid-back approach to the issue — simply waiting for a threat to present itself before wondering how to deal with it — they now need to adopt a much more proactive approach that leaves them prepared for any potential incidents.

The best way for businesses to protect themselves is by creating an incident response plan — a pre-determined strategy that must be followed by all employees within the business in the event of a cyber attack. It’s often the aftermath of an attack that causes the most damage, but these plans help businesses minimise that risk.

What should be included in an incident response plan?

Before businesses even sit down and think about how their incident response plan might look, it's important to understand that these should not be simple 'copy and paste' jobs: they need to be unique and tailored to the working nature and operational requirements of your business. If these aren't considered, the plan holds minimal value.

The first thing that any incident response plan should include is a list of any and all cyber threats that business could be faced with, whether it's a data breach, a DDoS takedown or a ransomware attack. On top of this, businesses need to consider their ways of working and how these might affect their chances of being targeted by online criminals. For example, if a business has employees that are frequently travelling on business trip or making visits to client's offices, they need to take into account the increased risks that they face through the use of unsecure Wi-Fi networks, using their work devices in public places, carrying confidential information on laptops or USB sticks, and other similar issues.

The plan should also include a list of the business' most valuable assets and clearly state where these are located, whether those assets are virtual or otherwise. Once listed, the plan must consider the risks that would be posed if those assets were to be seized during an attack. It can be extremely time-consuming to include all of this information, especially if your business holds lots of valuable assets, but it is an absolutely crucial part of any effective incident response plan.

Once all of this has been mapped out, businesses then need to think about the ways in which they should react and the steps they need to take in the event of a cyber attack.

The six steps of any incident response plan

With the foundations of an incident response plan now in place, there are six steps that need to be considered if businesses are to ensure that the plan is effective:

- Identify the incident — the first logical step when faced with any cyber attack is to find out what kind of attack it is. This can usually be identified through the monitoring of IT systems, employment of cyber intelligence and looking back through log alerts.
- Define the impact — once the attack has been identified, you then need to evaluate the potential damage that it has caused to your business. Check for any assets that have been stolen (this is when it's helpful for all employees to know the location of these assets), assess whether any data has been seized and pinpoint the timescale of the attack itself.
- Communicate — it's essential that all employees are made fully aware of the attack at this point. As part of the incident response plan, there should be a clear communication plan that encompasses various physical and virtual mediums and gives employees clear instructions on what they need to do following the attack.
- Gather the data — now that the business has a good understanding of the incident they've suffered from, all evidence must be collated and kept for reference, as this could prove to be useful in the days or months following the attack. Contact must also be made with the relevant authorities to make sure they're aware.

- **Begin recovery** — only at this point - once the nature and severity of the attack is totally clear — should businesses start the remediation process. This step must be carried out on a case-by-case basis, but common steps involve the resetting of passwords and the strengthening of IT infrastructure security measures.
- **Review** — once the threat has been addressed and operations are back to normal, businesses need to look back at their incident response plan and see where improvements can be made. Sometimes the best way for businesses to learn is through making mistakes.

Importantly, once a strategy has been created, you also need to make a long-term commitment to making sure that it's properly maintained and implemented. There's no use putting all the hard work in if it just sits neglected in a drawer for the rest of its life; the responsibility falls to the business to conduct regular reviews of its incident response plan to ensure it covers all eventualities.

Even if the threat of cyber attacks seems non-existent at this point in time, it is dangerous for any business to assume they are safe from harm. This is why, in order to minimise damage and mitigate risk, every business should have an incident response plan.




Link to the original article:

<https://www.itproportal.com/features/why-all-businesses-needan-incident-response-plan/>

Wavex Technology Limited

 70 Wilson Street, London

 020 7030 3210

 tellmemore@wavex.co.uk