ramsac
the secure choice

Action plan:

What to do in the event of a cybersecurity breach

What to do when a breach occurs...

It is inevitable that at some point an organisation will be hit by a cyber-attack or breach. It is important that all members of your organisation, from the employee who joined the organisation only yesterday right up to your CEO, know what to do in the event of a suspected attack. So, what are the steps you should take as soon as an attack is spotted and once the dust has settled?

We have provided a high-level Action Plan which breaks the response to a potential breach into 3 main areas, complete with recommendations of steps you should follow as the breach progresses:

Reacting to a suspected breach or attack

Your employees should know what to do in the event of a suspected breach or cyber-attack. The best way to prepare them is to create and share an Incident Response Plan (IRP). This should be very high level with simple steps to follow, and then supplemented with clear instructions for the Senior Leadership Team (SLT) or Incident Response Team (IRT) to deal with the aftermath. In general, this is how your employees should respond:

1 Isolate the device

As with most emergencies speed is of the essence, the faster your employees can respond to a potential breach, the less damage you can expect to your organisation.

If your employees see anything suspicious, such as unusual e-mails being sent in Outlook, files being inaccessible or encrypted, the mouse cursor moving on its own, these could be signs that their device has been compromised.

The first, most important step is to isolate the device from the network and the internet. This can be done by putting the device in Flight-Safe mode, turning off WiFi or un-plugging a physical LAN cable. By disconnecting and isolating infected devices as quickly as possible, it may be possible to prevent malware from spreading further throughout the organisation. DO NOT turn off the device – it is important to isolate, not turn off, as this will help preserve evidence of an attack and avoid permanently damaging the device.

If your organisation utilises servers, you will need to ensure there is a plan for how to isolate these from the network (either physically or virtually) during a suspected attack. Similar advice applies in attempting to isolate these from the network instead of shutting them down – but if you see files being encrypted across large numbers of devices, this could indicate a ransomware attack, so do whatever you need to do to get those devices isolated.

2 Raise the alarm

So hopefully a cyber-attack has just been stopped in its tracks! The next step is to raise the alarm to the right people. In most cases, your employees should be expected to report the incident immediately to their line manager and your IT team or helpdesk. They should tell them exactly what they experienced and what led them to believe it could be a cyber-attack. Encourage employees not to delay raising the alarm, as any delay could significantly increase the amount of damage done to your organisation.

Their manager will need to report the incident up the chain to invoke your organisation's formal Incident Response Plan (more on this later).

Your IT team will ask the employees more questions to ascertain if anyone else is impacted, whether they had any removable media connected or what they were doing at the time they noticed something suspicious, for example opening an email or browsing a website. Encourage them to be as open and honest as possible, as it is important your IT team can identify the cause of the attack.

3 Stay alert

Your employees will need to be told to stay off their devices, including any work accounts or apps they may have on mobile devices, and await further instruction from your SLT. You should consider what they can do now they are unable to use their IT systems. This is where a Business Continuity Plan is really important (more on this later).

Dealing with the attack

In the aftermath of a cyberattack, swift and decisive action is crucial. The steps you take in the first hours of discovering a breach can make all the difference in limiting damage, protecting sensitive data, and restoring normal operations. Now is the time to initiate your response plan, ensuring everyone knows their role and how to proceed during this critical period.

4 Incident reponse plan

Now that an attack has been reported, your organisation should invoke their formal Incident Response Plan (IRP). This is a document that clearly outlines how the organisation should respond – who to contact to deal with the attack and how to manage employees through the incident. Generally, this will start with a convening of your SLT or IRT members.

Some of the things that you will need to consider once an attack has been reported include:

- What other steps need to be taken to prevent the breach from spreading? For example, do all staff need to disconnect and log out of their devices, or do you need to disable a local network?
- Has the incident been reported to your IT team or helpdesk? Follow their advice to further safeguard your organisation.
- What do you need your employees to do now or know about the incident, and how should this be communicated to them (especially if they no longer have access to their devices!)?
- If client services are affected, what message do you need to get out to them? Notification of service interruption is of course important but consider what the message is if you haven't yet confirmed the scope or nature of a potential attack.
- This could be a significant impact to your employees and clients, so now is the time to review your Business Continuity Plan (BCP). Your BCP should outline how you can continue to operate services to customers as best as possible when some or all of your systems are unavailable. Depending on the services you offer customers, this could be fairly straightforward for employees or incredibly impactful, so consider the support they will need to continue to deliver services.

5 Reporting the incident

If this is a confirmed cyber-attack or breach, it is likely you will need to report the incident to various bodies. This should be done as soon as you confirm the breach.

- **Your insurance provider** – if you have business interruption insurance that includes impact from a cyber-attack or dedicated cyber insurance, you should report the incident to your insurance provider immediately. It is likely that your policy includes support from a cybersecurity specialist firm who will help you with containment of the breach, forensics investigation to identify the entry point, and then clear up and restoration of services.

- **Action Fraud** – Action Fraud is the UK's Policing body to report a cyber-attack or a breach. They can offer specialist advice 24/7 to help you deal with the immediate attack, as well as recording the breach as a crime and launching their own investigations.

- **Information Commissioners Office (ICO)** – if you suspect client or employee data has been accessed illegally or stolen, this must be reported to the ICO within 72 hours of you identifying the breach. Delaying reporting can result in significant and hefty fines.

- **National Cyber Security Centre (NCSC)** – the NCSC is the UK Government's body to prevent and tackle cyber-crime across the UK. By reporting a breach or attack to them, you are helping them to build up a picture of the threat landscape at a national level and be in a position to offer advice to other organisations.

6 Follow specialist advice

You have reported the incident to all the necessary parties and your employees know what they need to do to keep your business running as best as possible.

Now is the time to follow the specialist advice from your IT team and cyber specialists drafted in to restore services. Recovery from a cyber attack can be a lengthy process, anything from a couple of hours to a couple of months depending on the severity of the attack and how complex your IT environment is.

Keep employees and clients up to date and be as open as possible – it is much better to be in control of the situation and manage any potential reputational damage. If customer data has been accessed or stolen, you are legally obliged to report this breach to them. Not to mention, the ICO are a lot more lenient on fines for breaches where organisations have acted with integrity and responded appropriately to the breach, rather than try to cover everything up.

The aftermath

You're out the other side – the breach has been officially closed, your employees are (largely) back to work, and things can return to normal… right?

Of course, the last thing you want is to waltz back into another impactful breach. The following steps are important to try and prevent this from happening.

7 Debrief of the attack

You should pull your SLT or IRT together for a final debrief of how the attack unfolded and how you and the organisation as a whole responded. Some of the key things to discuss include:

- Did your employees know what to do when they identified the attack? If not, what further training is needed to either help them spot the attack sooner or know what they should do when it happened?
- Are there any changes needed to your Incident Response Plan based on how your SLT/IRT responded? Did everyone know what their role was and was the effort coordinated?
- If you had a Business Continuity Plan, did it work as intended? If you didn't have one, is it worth creating one!
- Do you understand all the subsequent impacts of the attack, such as what has been reported to the ICO, your insurance provider and your customers, and any potential legal ramifications?
- Any other lessons learned and what would need to be considered or improved in the event of another attack.

8 Prevention is better than a cure

Ideally, you want to avoid having to invoke your IRP or BCP at all costs. The best way to do this is with a layered protection from cyber threats. Some of the main things you can do to protect your organisation from attacks are:

- **Know your weak spots** – have a cyber specialist perform a full cyber audit and vulnerability scan of your organisation to identify potential gaps in your security and weaknesses that could be exploited by a cyber-criminal. Having this insight can significantly help you to prioritise the right cyber products or services that your insurance provider is now probably pushing you to take!

- **Security awareness training** – at all levels of your organisation, ensure employees know the signs of a potential breach and how to report it, and that your SLT know how to respond in the event of a future breach. This could also include phishing simulation training to help employees spot and report phishing attacks, which are one of the most common attack vectors for cyber-criminals.

- **Technical perimeter defences** – having a solid Firewall and robust Email-filtering/scanning and Anti-Virus/EDR products in place is of imperative importance. Not having these in place is like leaving the door wide open to cyber-criminals.

- **Account protection and security** – your employee's accounts should all be protected with secure passwords and Multi-Factor Authentication, and they should understand what they should and shouldn't do with their company accounts, which is normally stipulated in an IT Security Policy.

- **Cybersecurity monitoring** – as mentioned earlier, the quicker a breach is detected, the sooner action can be taken and the less damage that will be done. Having proactive 24/7 managed cybersecurity monitoring and response is proven to lower the impact of an attack and reduces the reliance on employees to spot a potential breach.

- **Backup and recovery** – data backups are essential for recovery following an attack, and these should be logically separate from the originals (i.e. a separate cloud backup). Furthermore, having a solid Business Continuity Plan is recommended so employees know how they can best continue to deliver services to customers if they are unable to use systems, minimising interruption to your business.

ramsac
the secure choice

How can ramsac help?

ramsac can help you with everything we have talked about in this Action Plan. For more information, please visit our website or contact us on;

Tel: **01483 412 040** | email: **info@ramsac.com** | web: **www.ramsac.com**

About ramsac

ramsac offers more than just IT support.

We assist clients in optimising technology – implementing, managing and supporting secure, resilient, flexible IT solutions. For many clients, we are the outsourced IT department, providing a strategic input, proactive management, 24/7 jargon-free support. With 30+ years of experience, we support end users, administer networks, secure data, and provide a named IT manager to visit onsite regularly. Our Cybersecurity monitoring tool, secure + is a fully-managed, 24/7 cybersecurity monitoring service, run by our dedicated team. Detecting breaches instantly, it prevents damage, ensuring peace of mind for our clients that their protected.

Whether designing new infrastructure, migrating to the cloud, implementing enhanced security practices or providing 24-hour IT support, ramsac manages IT comprehensively, so our clients can focus on achieving their goals, safe in the knowledge that IT is secure, staff are working efficiently, and the IT investment is delivering tangible benefits to the business.

Tel: **01483 412 040** | email: **info@ramsac.com** | web: **www.ramsac.com**