Action plan: What to do in the event of a cybersecurity breach

ramsac
the secure choice

Introduction

We are inundated with information on how to prevent becoming the victim of a cybercrime, however chances are now high that most organisations will fall victim to an attack sooner or later. So what happens next? What are the steps you should take in the immediate aftermath and once the dust has settled? This guide focuses on the security breach being a malware attack, but elements of our advice are relevant for all types of breach. As a minimum we would hope all organisations are as prepared as they can be to withstand a breach, but we have compiled the following list of actions should you be the victim of an attack.

Immediate actions

Raise the alarm

As with most emergencies speed is of the essence, the faster the alarm is raised and your staff get help, the smaller the Impact.

If you see anything suspicious, such as unusual e-mails being sent in Outlook, or a ransom note appearing, your machine may have been affected by malware, turn it off and raise the alarm immediately with your IT department or IT support provider. By disconnecting and isolating infected PC's as quickly as possible you may be able to prevent the virus spreading throughout the company.

Ransomware which encrypts data and demands a ransom to decrypt it takes time to go through and encrypt your files, but the ransom note often appears near the start rather than at the end. If you turn off your machine it won't be able to spread and start encrypting files on the network. DO NOT just shut it down, go home for the day and assume all will be well in the morning, as when you come in and turn it back on, it will just continue to encrypt more files.

Your support department or provider may advise you to disconnect potentially infected computers from the network by removing their network cable, as that reduces the risk of spread if someone accidentally turns it back on. It may be necessary to disconnect servers from the network, again to reduce the risk of malware spreading. This obviously will leave you with no IT systems, so you will need to turn to your Business Continuity Plan which should mean you still have access to backup business critical systems held off-site or in the cloud.

Communication is key

In the days of social media and the immediacy of all news, it is important to be open about a breach, certainly internally you should communicate to all employees as soon as possible to make sure they are all aware, that they take action if needed and they are vigilant to potential attacks. It may be necessary to communicate externally to partners and customers if they are at risk of being impacted by the breach. If there is no immediate danger you may want to wait to communicate out to them until after breach is dealt with.

Next steps

Do some detective work

Once the immediate risk of spreading has been removed, it is time to find out what has happened and how. To do this you will need to record as much information as possible about the incident, what you were doing at the time, any websites visited, e-mails opened etc. The more information you have, the quicker your support department can find the source and get everything restored and working again. In the vast majority of cases it is possible to trace where the malware first appeared. Honest information from users is key here as it allows your Support team to focus their efforts in a particular area. Obviously they need to make sure that they don't clear the malware and restore data, only to be re-infected as soon as they bring the systems back on-line.

Clean infected machines while still isolated.

Once the infected machine(s) has been identified, your IT department will start by cleaning those, usually using several different anti-malware products, as sometimes a piece of malware isn't detected and cleared by one product, but is detected by another. Some malware will bury itself deep down inside Windows, so depending on the malware in some cases it is necessary to wipe and rebuild infected PCs.

Scan all systems with extra anti-malware products.

While the infected machines are being cleaned or rebuilt, it is also necessary to scan all systems on the network, again ideally with several different anti-malware products so you can be sure it has not spread. This will give a good indication as to how many machines were affected and therefore how quickly the alarm was raised, which will be important in the aftermath when analysing how good your employees information security awareness is.

You will not be able to bring systems back on-line until you know the source of the malware. If the malware came in via an infected e-mail attachment which someone opened it is important to make sure that e-mail is removed from deleted items, archives, backups etc. However if the malware came in through a weak password you will need to review password policies, firewall rules, and perhaps reset all user's passwords. Finally you also need to consider any remote users who might have VPN access, and so could also be infected.

Bring systems back on-line

Once the above steps have been taken, you will now be ready to bring systems back on-line, often starting with critical users and then working round other users. Bear in mind that this may be several days after the initial malware infection, even for an infection which is limited to a small number of machines. It is time consuming to visit every machine, as the network is usually shut-down so the scans need to be started by hand.

Call the Police

Cybercrime is a crime! This may sound obvious but it is often overlooked by people, maybe because of the remote nature of the crime or possibly they feel there is nothing the police can do. However this is an important step you should take if you have been the victim of cybercrime.

Call your insurance/bank

Some business insurances now come with cybercrime protection. Call your insurance company and check your policy. It is also worth taking notes of what steps you need to take to ensure you don't invalidate your insurance. if your bank account has been compromised, it's important that you speak your bank as a matter of urgency, to find out what can be done to secure your compromised account, and to find out if stolen funds are recoverable.

In the aftermath

Debrief/analysis of breach

When everything is back on-line it is important to bring all of the information together from users and the support team to analyse what happened. What was the malware? How did it get in? Did everyone act promptly? Could the infection have been prevented? Were there any lessons learned? What needs to be improved? Once you have done this you can make a plan for any changes based on the lessons learned and areas highlighted for improvement, and then review to ensure they are implemented.

Legal issues and owning the problem

You must consider if there are legal ramifications to the breach, your data may have been stolen, but as you already know, it's not only your data. Usually, in such an attack, data from multiple sources are retrieved such as your customers' information, your business partners' details or financial credentials from credit-card companies. You may be required to report breaches to the ICO, and you should make everyone (whose data may have been comprised) aware of the breach. The best way to do this depends on the size and nature of the breach. Larger companies you will have seen put statements and press releases out to advise the public, it may be you handle it by contacting customers, suppliers, partners individually by email, phone or letter, you could also put a statement on your website. It is important you are open about the breach to ensure any affected parties are aware, own the problem and make it clear you are putting policies in place to prevent similar situations in the future, invite affected parties to contact you to discuss their concerns.

Prevention is better than a cure

Your organisation has been the victim of a cybercrime, so after the dust has settled and the issues it created have been cleared up the most important thing to remember is there is nothing to stop it happening again so prevention is better than a cure! Our top 3 tips for prevention of cybercrime are;

1 Technical defences

The risk of attacks can be reduced by good configuration and systems, for example good quality, up-to-date anti-malware software, firewalls, good password policies and systems which are kept updated to close the holes used in drive-by attacks. However no matter how good the technical security there are always risks with brand new malware which might find new holes, and that the anti-malware can't block. Usually it only takes a few days for patches and anti-malware updates to stop those attacks, but there will always be periods where you're reliant on users as the first line of defence.

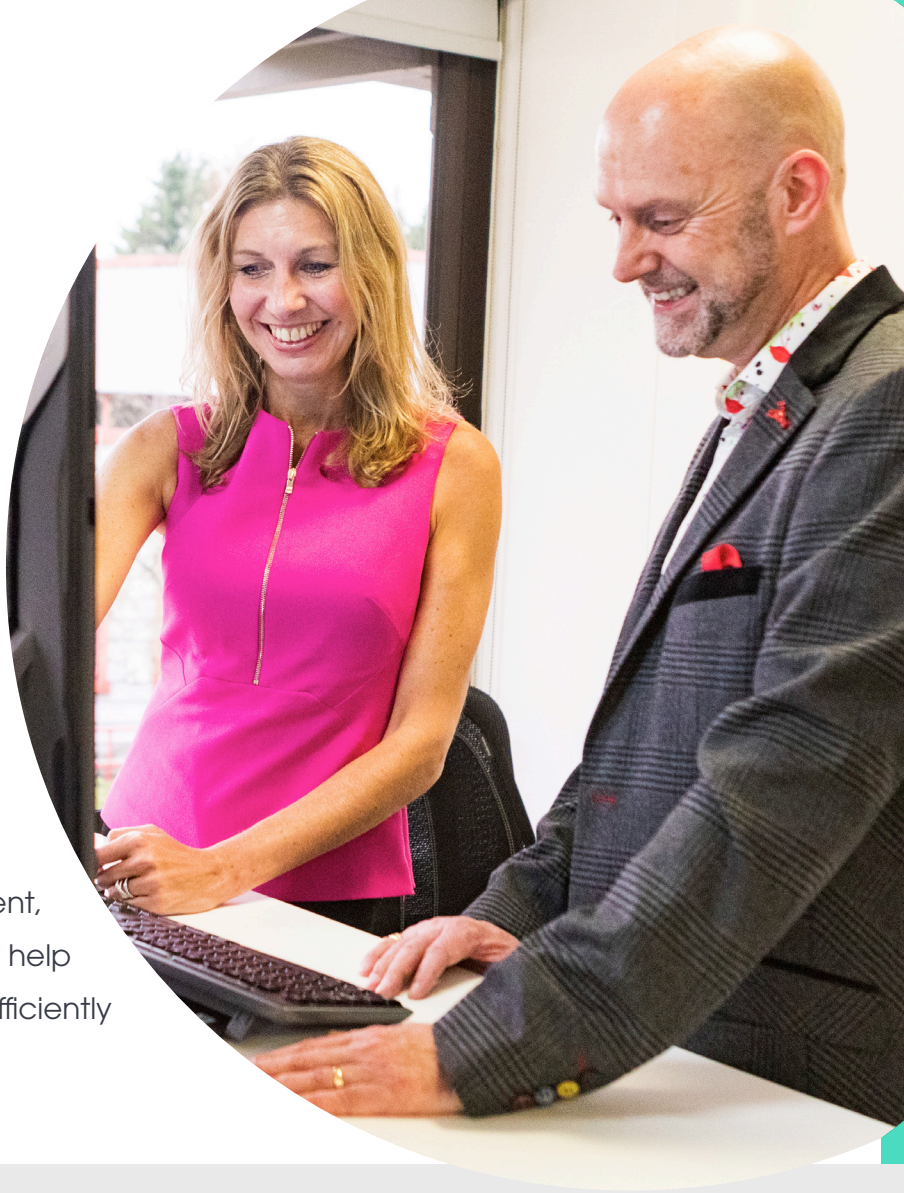
2 Cyber Security Awareness training

Users need education around being naturally suspicious of things that look unusual, in the same way as they will be for their personal security. If you see someone looking suspicious loitering near a cash machine most people would choose a different machine, raise it with a police officer, or at least take extra precautions to stay safe. Likewise, if a user receives an attachment from someone they don't know, or an e-mail written in an unusual way from someone they do know, those are the times to stop and speak to a manager or the IT support team. Looking at a few e-mails each month that look suspicious is far less work, and far less expensive, than spending several days clearing up after an infection.

3 Backup regularly

Unfortunately with ransomware which encrypts your files, and potentially those on the network, and then demands a ransom, usually the only way to restore data is from the most recent backup as it's virtually impossible to decrypt the files without the key. Therefore long before any incident, it is important to make sure you have complete backups, which have been tested so you know they can be restored. Also make sure that if you use hard-disk based (rather than tape or cloud) backup that there is also a separate copy in the cloud or elsewhere, as we have seen ransomware also encrypt hard-disk backups.

About ramsac



ramsac has a clear mission
- to be at the heart of IT

We help our clients to get the best out of technology – implementing, managing and supporting secure, resilient, flexible IT solutions.

We work with small and mid-sized organisations, providing them with strategic IT input, proactive management, jargon free IT support and solutions that help them to grow their own organisations efficiently and securely.

More information

This action plan is not exhaustive there may be additional steps you are required to take due to the nature of your organisation or the nature of the breach, however these are the main points you need to consider in the majority of breaches. The key to minimising problems caused by cybercrime is reacting quickly and decisively so make sure you and your employees are prepared to act in the unfortunate event of your organisation being targeted.

ramsac have a wide range of services to help organisations to improve their cybersecurity. We can help with all aspects of cybersecurity training, from board level briefings, end user training workshops and online learning portals.

Whether you're at the very beginning of your cyber resilience journey or are looking to take your cybersecurity to the next level, our Cyber Resilience Certification will help you do just that. With Bronze, Silver and Gold certification levels available, we'll conduct an audit to understand your current security status, cover how to strengthen your protection, and ultimately, show your customers and stakeholders that you take the protection of their data seriously.

For more information on protecting your organisation from cybercrime please contact ramsac on 01483 412040 or email info@ramsac.com.

ramsac Limited

www.ramsac.com
01483 412 040

ramsac
the secure choice