Cybersecurity: the basics

a ramsac guide

●ramsac
the secure choice

Contents

Introduction

Cybersecurity has fast become the business buzz word of the current decade. Once considered to be a risk that only large multinationals and government agencies needed to really worry about, today, every organisation needs to concern itself with the proper protection of information and the critical elements that support it, such as systems and hardware that use, store, and transmit data.

Not a week passes without major IT scandals or data breaches reaching the national news headlines, and with GDPR now in play, the fines for lost electronic data are now starting to be seen.

But this is not just about the high profile attacks that make the news headlines, this is about the stress, inconvenience, and often embarrassment that can be seen each and every day in SME organisations, when someone clicks on a malicious email link, or makes a payment to a fraudulent bank account, resulting in loss of data, lost cash, network downtime, staff disruption and perhaps worst of all, the reputational damage caused when you have to reach out to apologise to your own customers, for the poor housekeeping that has led to a breach of data or a reduced service.

There is no organisation that is not at risk. Cybercrime literally affects us all. As a business leader, it is your legal duty to ensure that you have taken appropriate preventative action to ensure that you have minimised the risks, trained your team, and agreed a plan for how to respond should you be the next victim of cyber criminals.

In this short white paper, we look at the key considerations that every leader should understand when it comes to protecting their organisation against cybercrime.

Creating a cybersecurity policy

It is no longer enough to think of cybersecurity as purely an IT issue. These days, it should be a company-wide concern that starts at the front door and ends with employees at home.

It may make sense to move from a product-centric to business-centric risk-management style view of security. With the emphasis now on processes and people, it's the perfect time to readdress security challenges with a fresh perspective and reconsider how best to manage and mitigate security risks.

Who is responsible for security?

Many organisations use a "grassroots" or bottom-up approach, with the responsibility for cybersecurity lying with systems administrators. While companies will benefit from the technical expertise of the employees involved, such an approach can still be highly problematic. This is largely because it can be difficult to gain wide participant support across the organisation, and there will often be a lack of staying power. There is a danger that if all the responsibility for and knowledge of your organisation's security processes lies with just one or two people, you may be left vulnerable should they leave the company, or even just be away for any reason.

A top down approach, initiated by upper management, is often far more effective. This affords security the respect that it deserves and demonstrates to the entire company that it is a critical issue.

GDPR regulations firmly assert that cyber security is a duty that the officers of your organisation cannot delegate – the whole senior team have to be seen to be leading on the plan to protect your organisation.

Increasingly, companies are employing top level security officers as members of the C-suite. However, for many businesses this is not an appropriate or realistic option. A suitable alternative approach may be to create a security committee, with each member responsible for a separate aspect of cybersecurity appropriate to their role within the organisation.

Your committee may include such personnel as: your head of IT, a member of the senior management team, your office manager, and department representatives. Depending on the resources and expertise available within your organisation, this committee can deal with security issues in-house or work with an outsourced IT supplier to ensure that the company is protected.

A constant concern

It is easy to decide a raft of actions, create a policy and then move on, but cybersecurity is an issue that must be frequently revisited, the policy revised in light of new dangers or opportunities. Furthermore, discussing the issues regularly will help keep everyone vigilant.

Those involved in security should schedule regular meetings to discuss any new concerns or issues and ensure that processes are running smoothly and nothing has been overlooked. A good way to keep your processes rigorous is by understanding a cyber essentials assessment.

Cyber Essentials

Cyber Essentials is a Government-backed and industry supported scheme to guide businesses in protecting themselves against common cyber threats.
The main objective of the Cyber Essentials assessment is to determine that your organisation has effectively implemented the controls required by the scheme, in order to defend against the most common and unsophisticated forms of cyber-attack. Cyber Essentials defines a set of five key security controls, which, better protect organisations from attacks. The UK government has said implementing the Cyber Essentials 5 security controls could prevent around 80% of cyber attacks.

Three pillars of cybersecurity

People

Human error accounts for almost 90% of cyber-attacks. Everyone within the company needs to be aware of their role in reducing the impact of cybercrime. This can be from handling sensitive data responsibly to knowing the difference between a safe email and a malicious email. Providing consistent training to employees on both cybersecurity and physical security is vital.

Process

A clearly defined cyber strategy needs to be implemented to reduce the risk of a cyber attack. Having policies and procedures in place will help employees know how to prevent or respond to cybersecurity threats. Processes need to be continually reviewed: as cybercrime is constantly changing and processes need to be adapted to reflect the new threats.

Management systems are the key to the second pillar. Without a clear management system in place, issues and data will fall through the cracks, making your entire company vulnerable to cyber security attacks.

Data & technology

Although human error accounts for a lot of cyber attacks it is still vital that an organisations technology is up to date. Ensuring patches and updates are installed promptly and Antivirus and firewalls are maintained. Using tools like mobile device management, allows organisations to remotely wipe lost or stolen devices. By understanding the risks to your organisation, you can determine the controls needed to minimise these risks and what technologies you will need to deploy to help you.

Awareness and training

According to the 2019 Ponemon Institute Cost of a Data Breach Report 51% of breaches are malicious and 49% caused by human or system error.

Even with the best security tools, incorporated into a robust and all-encompassing data strategy, things can easily fall apart if your staff are not aware of the issues and the part that they can play in mitigating them. From the moment that a member of staff joins your organisation and creates their first password, you should be working to make them someone who will strengthen your security, not weaken it.

Make sure cybersecurity is at the heart of your IT strategy, that internal financial processes are robust, and staff are trained to be vigilant and aware of threats.

In sight, in mind

Employee awareness is paramount. Your human firewall can make or break your cybersecurity shield, and your colleagues are at once your company's greatest assets, its biggest weakness and its best defence.

In addition to including your security policies in your organisation's handbook and induction materials, it is a good idea to schedule regular security awareness sessions to ensure that best practice stays at the top of employees' minds, everyone is aware of new threats and newcomers have ample chance to learn the ropes.

The most effective way of doing this is to deliver regular, short and relevant awareness training – focused on how and end users can impact on security rather than talking about complex techie solutions.

Online video based courses are probably the most cost effective way of awareness and training. However, as an organisation you should always consider people's different learning preferences. It may also be worth scheduling some in-person training sessions each year too.

First steps

There's no better time to implement or improve your cybersecurity policy.

Testing Times

It needn't be daunting. The first steps can be incredibly simple – just testing the current strength of your security and identifying any weaknesses is a great start.

The majority of breaches actually come down to human error, so a test of your employees' awareness and compliance with security best-practice makes a great starting point. We suggest a three-pronged approach, with a dummy phishing email sent out to your employees, a staged phone call in which you attempt to obtain sensitive information and an in-person attempt to get into the inner sanctum of your office by someone unknown to your colleagues.

Use available resources

You should also immediately make use of resources already available to you.

Always keep up-to-date with your security software messages and be sure to regularly access your control logs and keep abreast of any reporting systems you have in place. Be sure to act on any alerts your monitoring services issue.

Make sure you have the ability to see what software and services are running on your network and to identify anything that should not be there. Run regular vulnerability scans and penetration tests to scan your systems for known vulnerabilities, and make sure you know how to address any identified issues.

Get the ball rolling

Identify key personnel for your security committee, get a meeting in the diary and circulate an agenda.

Know what to do if something goes wrong

Even with the best security programme, well trained staff and the best will in the world, breaches may still occur. It's essential that you are prepared for this eventuality, discuss how best to react to a variety of scenarios and have a mitigation plan in place to help your organisation deal with the fallout of a breach and get back to business-as-usual as soon as possible.

It may be worth taking out cyber insurance, but good research is needed to ensure that you have the right type of policy for your business. It's also essential to treat this as an addition to a robust cyber security defence and emergency plan. Don't forget that it is impossible to insure against reputational damage, which can be fatal to a business.

Having a strong emergency plan in place can minimise the damage caused by a breach.

Simple tips to improve your cybersecurity

Online security

Trust your instincts online – if you feel that a website looks "off", avoid it. If something feels wrong about an email, delete, ignore or report it as appropriate.

Also:

- When you do visit a website you don't already know and trust, always check for "https" in the address bar – this lets you know your connection is secure.

- Be email-wary. Be especially cautious of messages that:
  - are from unfamiliar senders,
  - request personal or financial information over the internet,
  - aren't personalised,
  - try to force you into hasty action with frightening or upsetting information.

- Learn how to spot spoofed emails and be on the lookout for them.

- Keep web browsers and operating systems up to date.

- Install any and all security updates offered.

- Be wary of pop-ups – don't click on links or enter personal details into one.

- Use strong passwords – no "123456" or "password"!

- Consider using a password management tool.

Devices

Whether your device is company-issued or "bring your own", it has the potential to become a security risk for you and your organisation.

A few simple actions can minimise the danger though:

- Don't take a for-business device with you when travelling unless you are sure you need it.

- Back up your data, lock your phone, make use of apps such as "Find My iPhone" or "Android Lost" and enable remote access to protect and preserve your information if your phone or tablet is lost or stolen.

- Avoid rooting or "jailbreaking" your devices.

- Only download apps from a legitimate app store.

- Be discerning when choosing apps – app malware is a rarely considered but serious issue.

- Clear all data before exchanging, selling or disposing of your device.

- Ideally don't use public Wi-Fi rather ensure you have an appropriate data tarriff on your mobile device. If you have to use a public WiFi network – then you should use a VPN and adjust your device's security settings to limit access.

- Do not trust or use any USB devices without first having it checked and given the all-clear by your IT department.

Around the office

Many thieves and scammers often succeed by exploiting social behaviour such as compassion and politeness. Brazen thieves have been known to simply walk into an office as if they belong there and remove items unchallenged. Be aware of who is entering and exiting your workplace.

- If you have the infrastructure to support it, protect your office by implementing a mandatory sign-in and name badge policy for visitors

- Be vigilant to strangers – a simple "excuse me, can I help you?" can help verify identities, without any risk of causing offence.

- Be aware of USB key scams. If a member of your team were to find a USB key in reception or the car-park, what would they do with it?

  The correct answer is to throw it away in the bin.

- Don't leave valuables in clear view or in unlocked drawers.

- Close and lock doors and windows before leaving a room empty for any length of time.

- Don't share your office ID or leave it lying around.

- If you use a laptop, pack it away out of sight when you are not using it, keeping it with you if possible.

- Lock your PC screen whenever you leave your desk.

- Don't write down passwords and leave them lying around.

- Clear meeting rooms and wipe whiteboards/flipcharts after use.

Tips for remote working

- Keep all mobile devices with you whenever possible; never leave them in a car or hotel room (even in the safe)

- Only connect to trusted networks

- Use a strong password or a long PIN on your smartphone and tablet

- Minimise sensitive information you keep on your mobile devices

- If possible, use full disc encryption to make your laptop as secure as possible.

- Never use public Wi-Fi or computers when you are handling or working with sensitive information.

- Use your corporate VPN whenever possible.

Find out more

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. We can carry out an audit of your current set up and provide best practice advice on how to protect your organsation and finally we can help you to achieve the Government backed `Cyber Essentials Certification'.

To book an initial consultation:

Call: **01483 412 040**

Email: **info@ramsac.com**

Visit: **www.ramsac.com**

ramsac Limited

www.ramsac.com
01483 412 040

ramsac
the secure choice