Cybersecurity: the basics

a ramsac guide

ramsac
at the heart of IT

ramsac
at the heart of IT

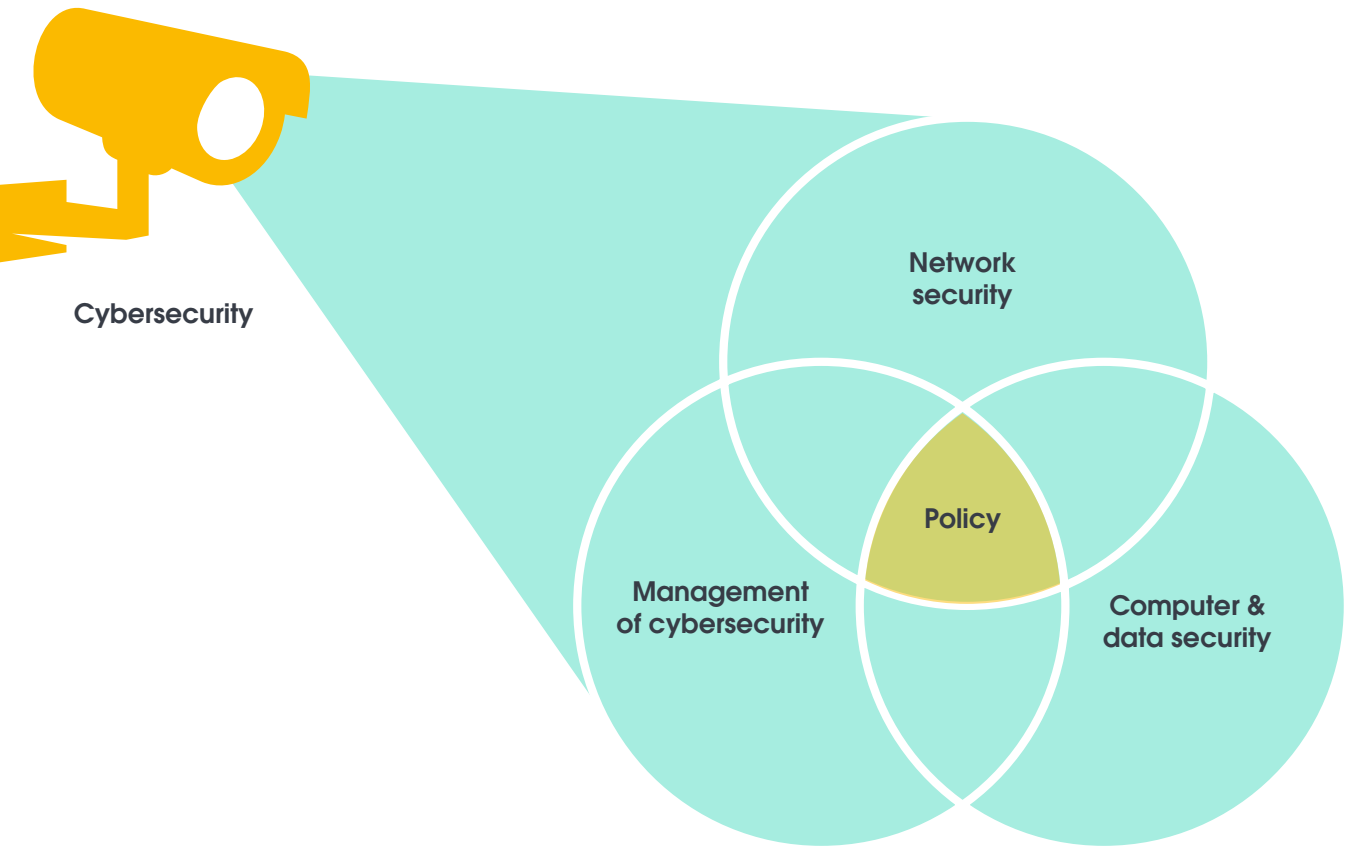
Introduction

Cybersecurity is the protection of information and the critical elements that support it, such as systems and hardware that use, store, and transmit data.

Thanks to the Internet, millions of computer networks are now in communication, many unsecured. This is a serious concern when you consider how much the ability to secure a device's data is influenced by the security of every other device to which it is connected.

Cybersecurity is an evergreen concern, but it has never been more pressing than now. Security breaches are on the rise and the average cost per breach can be ruinous.

Components of cybersecurity

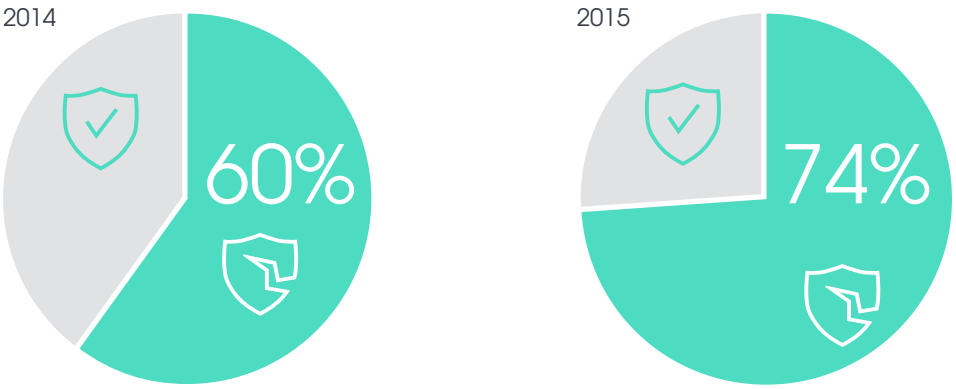


Who is at risk?

In short? Everyone.

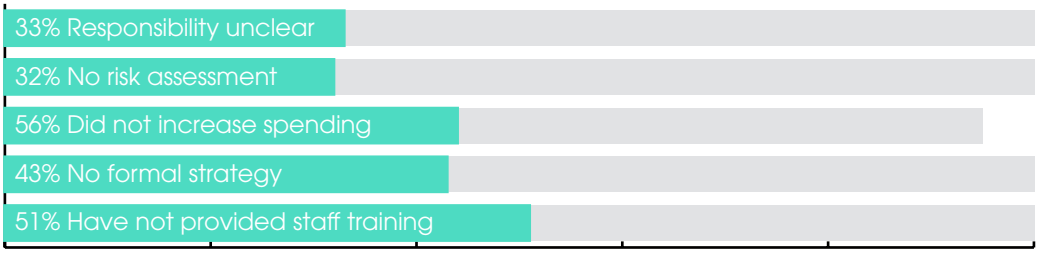
It's easy to assume that it's only big businesses that really need to worry about security breaches – surely small organisations can just fly under the radar?

Small business data security breaches



Over the course of the last year alone, 74% of small businesses experienced at least one security breach, with the median number of breaches per organisation coming in at 4. This is up from 60% in 2014, and the figures are expected to keep escalating.

Large organisations data security



However, 33% of large organisations said "responsibility for ensuring data is protected is not clear" and 32% of all respondents in 2015 hadn't carried out any form of security risk assessment. Meanwhile, only 44% of organisations had increased their security spend in 2015.

A similar picture emerged in The Institute of Directors Cyber Survey 2016, in which only 57% of respondents said they had a formal cybersecurity strategy, and only 49% provided training for staff.

What is at risk?

Catastrophic costs, loss of customer trust and a great deal of wasted time are all potential consequences of an cybersecurity breach, and each can be devastating to your organisation.

Average cost of the year's worst security incident

£1.46m - £3.14m	£75k - £311k
to a large organisation	to a small business

In their 2015 survey for HM Government, PwC discovered that the cost of breaches suffered by those surveyed had soared, with the average cost for the year's single worst breach coming in at £1.46m - £3.14m for a large business and £75k - £311k for small businesses.

Not-for-profits, education and the public sector

For charities, education providers, and the public sector, the onus to avoid security incidents is perhaps even stronger. With every penny needing to be accounted for, a breach represents an untenable financial hit. Furthermore, these groups experience increased pressure to avoid reputational damage, and security incidents can be devastating.

The immediate costs are not necessarily the most painful aspect of a security breach though. The damage to an organisation's reputation can be irreparable and devastating. In fact, reputational damage was the most commonly cited answer when the organisations surveyed were asked what the key factor was in their worst breach of the year.

Breaches can affect anyone at any time, and so a robust cyber security strategy, encompassing well implemented processes is essential for every business, regardless of size or sector.

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.

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.

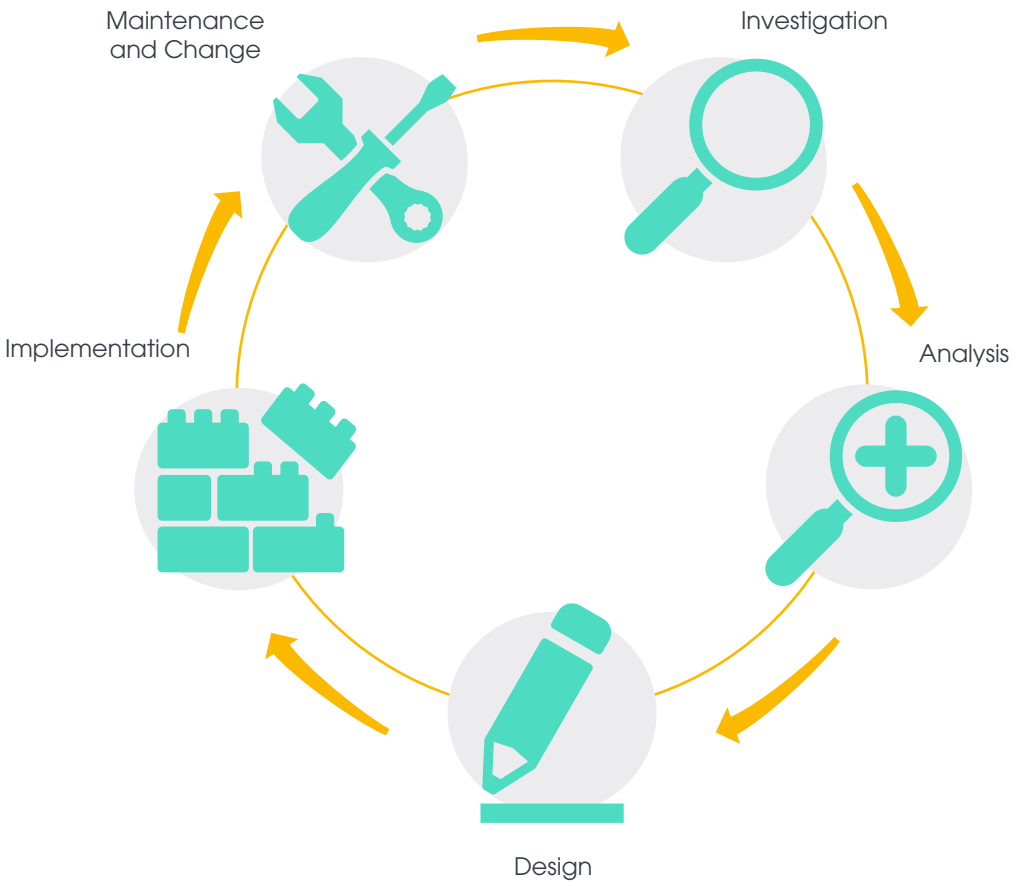
Your committee may include such personnel as: your head of IT, a member of the senior management team, your office manager, and department representatives. Depending on the resources and expertise available within your organisation, this committee can deal with security issues in-house or work with an 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 referring to the systems development lifecycle, or SDLC.

The systems development lifecycle



The SDLC is a methodology for planning, designing, testing and implementing an information system.

It can be applied to the creation and maintenance of your organisation's cybersecurity processes to help you ensure that your approach is rigorous, with no gaps or key vulnerabilities.

Investigation

In the investigation stage, you'll want to identify your security goals and discuss the process needed to achieve these, along with the project's constraints. Your goals may include infrastructure and technology requirements, or personnel goals (such as increased cybersecurity awareness) – or, most likely, a mixture. You should also perform an "organisational feasibility analysis" to identify resources you already have available to help protect your information, as well as your ability to access others you might need.

Analysis

During this phase, you need to analyse your existing security policies or programmes, along with documented current threats and associated controls, referring to any documents you created during the investigation phase. You will want to consider any legal issues that might impact your security solution.

Design

Now it's time to actually create and develop your cybersecurity plan.

Your plan should include:

- Continuity planning
- Incident response
- Disaster recovery
- Staff awareness training

Elevate any security technology you already have, decide what new elements you need and look for possible alternatives. Also consider any personnel issues that may arise from new technology procedures you may implement.

You'll want to perform feasibility analysis again at this point to help you decide whether you can roll out the programme in-house or you'll need to outsource elements.

Implementation

During this stage, you should acquire any necessary technology, test it, implement and then test again. Any relevant training programmes should take place at this stage. The stage ends with the entire tested package presented to stakeholders for final approval.

Maintenance and change

As ever more sophisticated cybersecurity threats emerge and older dangers evolve, your organisation's security profile must mature and adapt.

Having cybersecurity policies in place is crucial, but there is no point creating policies that are incomplete, poorly thought out, unsuitable, superfluous, or ignored by users. Rather than trying to solve all your cybersecurity concerns in one go, you should view policy development as a carefully planned, continuous process requiring constant commitment. The life cycle approach can be a good way to achieve this.

Awareness and training

According to the PwC survey, 75% of large organisations and 31% of small businesses suffered staff related security breaches in the last year.

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.

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 sight, in mind

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.

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.
- Limit your behaviour and the business you conduct when connected to a public WiFi network – use a VPN if possible 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.
- 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.

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
- Deactivate Bluetooth and wireless when not in use
- 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.

ramsac Limited
Godalming Business Centre, Woolsack Way
Godalming, Surrey
GU7 1XW, England

www.ramsac.com
+44 (0)1483 412 040

ramsac
at the heart of IT