CYBERSECURITY AND THE CLOUD
7 ACTIONS YOU CAN TAKE TO STAY SAFE

Many businesses and organisations have been cautious about shifting some or all of their software and IT infrastructure to the cloud because of concerns regarding cybersecurity.

The loss of direct control about how services are provided can be worrying, particularly as under regulations such as GDPR you still are accountable when things go wrong.

Cyber security is always challenging, but many smaller organisations find that shifting their services to reputable cloud services providers has actually improved their cyber security. The loss of control is outweighed by the fact that the large cloud vendors have the technical expertise and resources to allow them to invest heavily in ensuring they and their customers are safe.

They key to staying safe it the cloud is to be diligent – do your research to ensure that prospective cloud providers, whether they are providing a Software-as-a-Service (SaaS), or Platform or Infrastructure-as-a-Service solutions, have the skills and resources to keep your data and information safe.

Below are 7 actions you can take to make to be sure your organisation is cyber-secure when using cloud services:

1.

Do a cloud data inventory

Regularly inventory the data you are using or storing in the cloud, and check that both you and the cloud services provider are protecting it appropriately.

Certain types of data have special types of protection mandated by regulation or by certain industry bodies, and you need to take this into account when doing your inventory. For instance, the personal data of EU citizens has been granted special protection through the General Data Protection Regulations, and payment card processing on-line is governed by the PCI Security Standards Council, established by the major card providers including Visa a
nd Mastercard.

If you don't know what's in the cloud, you can't be sure it's protected properly!

2.

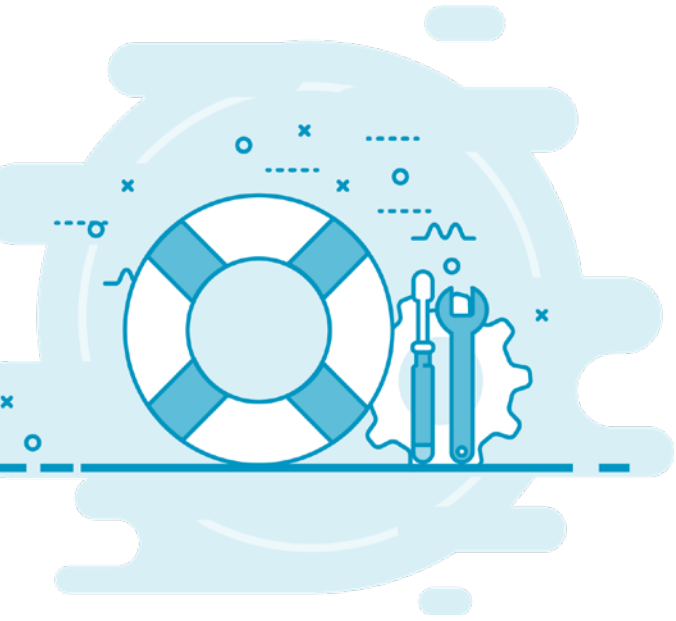
Do your vendor due diligence

When considering whether to sign or renew a contract with a cloud vendor, do your due diligence to make sure they themselves are cyber aware.

Ask the supplier what accreditations and certifications they have and ensure that these are appropriate for the type of services they are providing and the type of data they will be storing or processing for you. There is a plethora of international, national and vendor-focused accreditations and certifications, such as ISO27001 (the International Standard for Information Security), ISO27017 (the Code of practice for information security controls based on ISO/IEC 27002 for cloud services), Cyber Essentials (in the UK), PCI-DSS certification for those providing online payments etc.

Many small SaaS vendors provide services which themselves are platformed on larger cloud providers such as Microsoft Azure, Google or AWS. Where possible, try and understand the cloud services provider's own supply chain and ensure that they and their staff have the appropriate accreditations and are competent when developing and providing services on these platforms.

A supplier which is open about how they manage their own cyber-security and is willing to submit itself to a 3rd party audit to obtain appropriate accreditations and certifications is more likely to keep you and your business safe.



3.

Have a backup plan if something goes wrong

One of the benefits of cloud services is that the supplier is often able to provide higher levels of availability than you own internal teams - their size means they are able to invest in the up-to-date technology and staff required to provide outstanding levels of service. Nevertheless, outages still happen, so it is important that you have a 'business continuity plan' to ensure that, if a key cloud service goes down for a few hours at the busiest time of year, your business can cope.

It is also not uncommon for cloud vendors, particularly those providing niche services, to go bust. Again, ensure that you have a plan in place for getting your data out of your cloud services at short notice and regularly assess which services you are using to identify the point at which a once 'experimental' cloud service is now business critical. If this happens, assess your options – is a larger, more robust cloud vendor available? Should you consider putting the software into some sort of escrow, so it continues to be available to you if the software vendor fails? Should you even consider acquiring the software vendor? Of course, this has the added benefit of keeping business critical software out of your competitor's hands!

Take the Scouts' motto to heart and always 'be prepared'.

4.

Protect your 'Edges'

The places where the 'edge' of your own IT infrastructure meets the 'edge' of the cloud services can be a point of particular vulnerability. Keeping your 'edges' secure is a critical part of good cyber security. Here are some areas to focus on:

- Implement good asset management so you know what devices you are using and can ensure they are patched and maintained properly.
- Switch your firewalls on and install anti-virus on all laptops and desktops, and switch on password protection for all devices.
- Encrypt hard drives and make sure that lost or stolen mobile devices can be locked and remotely wiped.
- Discourage staff from connecting to public wi-fi hotspots – encourage them to 'tether' their laptops using their mobile devices or provide a wireless dongle. If you are a larger organisation, consider providing a 'virtual private network' (VPN) for staff when they are working remotely.

Another type of 'edge' to consider is how you control access to your cloud systems. Everyone knows that staff should never share passwords, but too many people still do it! Not only does this cause significant cyber security issues as you have no idea who is doing what to your systems, but in many cases, it is also illegal!

Larger organisations may wish to implement centralised access controls, also called 'single sign on', which channels logins for all applications (including SaaS applications) through a single point. Not only does it mean your staff only require a single password to access all the systems they need, but it also simplifies your joiners and leavers process.

5.

Educate your staff

Even the most well-meaning of staff can pose a security risk if they are not aware of their cyber-security responsibilities and are not educated to understand and manage the risks they face every day.

Make a single individual accountable for implementing cyber security within your organisation. A critical part of their job is to make sure that everyone is pulling their weight when it comes to keeping the company safe, including the development and publication of an acceptable use policy which all staff must read and comply with. This policy should outline staff responsibilities for how they use the technology services you provide them, including their use of cloud services. As an example, you may wish to forbid staff accessing private email accounts and social networks from work devices or from using public wifi. Breach of the acceptable use policy should be considered a disciplinary offence and staff should be regularly reminded what they need to do to comply with the policy.

Your staff should also receive education about cyber security in general, such as how to recognise phishing and 'social engineering' attacks (where staff are conned into revealing secure information including passwords), as well as being alert for email attachments or USB memory drives infected with viruses.

Your technical staff will need a deeper level of education regarding how to identify and fix up cyber security vulnerabilities, and what to do if a breach does occur. You also need to ensure they have the resources and training they need to ensure your computer systems are kept up to date and that your 'edges' are kept secure.

Consider whether there is any requirement for specialist cyber security training for technical staff in their professional development plans, or whether it might be worth partnering with a 3rd party partner to help you get things right.

6.

Consider obtaining your own cyber security accreditations and certifications

Even some very small businesses find the investment in obtaining their own cyber-security accreditations is worthwhile. Achieving and maintaining ISO27001 certification or participating in a national certification scheme such as Cyber Essentials in the UK can provide confidence for your own customers that you are keeping their data safe.

While many small business owners might dismiss the effort involved in preparing for and achieving these certifications as being too onerous, they are designed so that even the smallest of organisations can obtain them. This is because they are focused on ensuring organisations assess their own risks and take proportionate measures to manage the risks. The emphasis is what works for each individual organisation. For small businesses and organisations this means a focus on ensuring cyber-security is embedded in the practices of the entire organisation rather than developing shelves of processes and policies which no one ever looks at.
Cyber security certifications really do help win and retain business, and even the smallest of organisations can and have become certified.

7.

Get an external 3rd party to test your defences

Many commercial organisations provide services that try and identify potential vulnerabilities within your own software and infrastructure, where your internal services meet cloud services, and of the cloud services themselves. This type of test is called ‘penetration testing’ and is designed to identify weaknesses in your security so that any issues can be resolved. There are many reputable cyber security organisations providing penetration testing, but as with any supplier or vendor, do your supplier due diligence to ensure they are themselves qualified to carry out this type of testing, and that they employ reputable ‘ethical hackers’. Ask for references for other organisations of your own size that they have helped and do make sure you actually contact the references to hear what they have to say in person, rather than just trusting what the company says about their own services!

Keeping your business or organisation secure as you move to the cloud can be daunting, however implementing these 7 actions will help you make the transition safely. In fact, as stated in the introduction, many organisations find that their security is actually improved as they move to the cloud, because large cloud service providers have the depth of expertise and resources that smaller organisations lack.

Cyber security is everyone’s business, so make sure that your staff and anyone else who accesses your systems are aware of their responsibilities, and that you ensure you invest the time and resources needed to make the transition to cloud safely.