7 Steps to Improved Cyber Security for Smaller Firms

abbey ICT

IT • Cloud • Telecoms

Britain's response to Russia's illegal invasion of Ukraine brings with it the threat of retaliatory cyber attacks

Whilst this threat has been highlighted by the Home Secretary and head of the Government Communications Headquarters (GCHQ) the guidance issued to businesses is not particularly helpful to smaller firms. This document is an an attempt to fix that and make cyber security advice more accessible for SMEs.

It might be your least favourite topic, but burying your head in the sand won't serve you well

This is probably one of the most unpopular topics for those who don’t know much about it.

We all know it’s a risk to us either personally or professionally, but unless you are interested in the subject or acquainted with some of the terminology, it’s a tough topic to tackle.

We wanted to write a short guide highlighting some of the key areas a business should address to improve its cyber security.

It is meant as a guide and not a definitive list of “Do’s and Don’ts” however, if the areas covered are addressed, your business will be more secure.

1. Awareness

Cyber Security isn't just a problem for your IT team or IT service provider, although they will certainly help build awareness.

Most threats are aimed at normal users. A fake website, an email pretending to be someone you might know or trust, or a text message are the most common starting points.

With these they have access and this can soon spiral from a single user through to the whole company.

Training everyone in your organisation to look for the common signs is one of the most important steps in protection.

2. Login credentials

Passwords haven't been the name of your pet for a very long time, thankfully, however people still use things such as “12345”, “Password”, “Qwerty”, “abc1234”, “sports teams”, “birthdays”, and variations around the theme.

A seasoned hacker will crack these within seconds.

Complex passwords based on things you see around you when setting passwords (such as phone-CHAIR-door) are harder to guess.

Secondary authentication methods such as One Time Passcodes (OTP) are now commonplace and should be used to delivery extra security.

Password policies controlling complexity (minimum length, character types), lockouts following incorrect login attempts and, arguably, forced changes are an important step helping to ensure if a username gets into the wrong hands it's more difficult for outsiders to gain access to your systems.

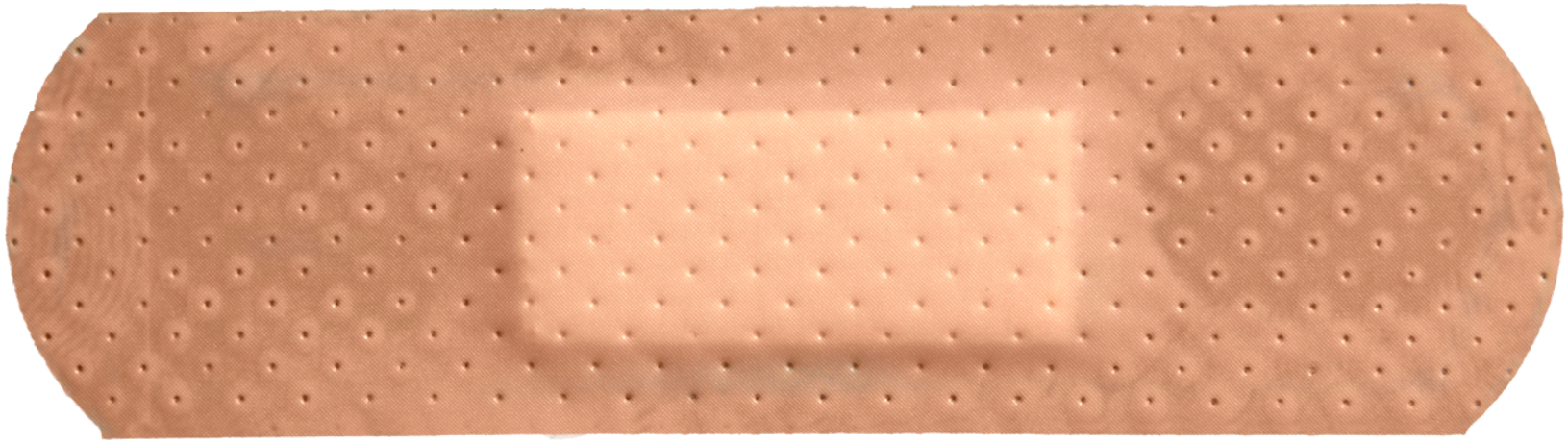
Use different passwords for different systems and make sure nobody shares them!

3. Updates

Ensure you implement system and application updates, not just your operating system and antivirus products but all of the apps you use.

Your IT provider can help with this and should already manage this for you in line with the business needs. If you aren't sure then ask them.

It matters because new vulnerabilities come to light all the time, and as they do, software providers issue security patches to overcome them.



4. Backups

Again not just a topic for IT teams and your service provider to discuss.

All IT teams will look to provide backups to give the business the best resilience from any potential loss.

Remote site,
Cloud backups and a design with air-gapped solutions (offline) are commonplace.

If you aren't
aware of the backup strategy and it falls into your remit, then ask those who manage it.

As a user you have a part to play too.

Making sure your data is saved in the correct location ensuring the backup strategy functions correctly is important.

If you are unsure ask your IT provider for clarification.

5. Data security policies

Think about what you store, where you store it and who has access to it.

Protect your most important data first, allowing only those who need access to it to have it. Be aware of the legal guidance and controls.

There are a great many options to help control data in today's cloud environment including once that data leaves your environment, which can be useful when you are sharing it with third parties.

Think about your devices and physical access too. If someone is able to walk into your office and access the systems or pick up a laptop and walk away with it, what is at risk? Local disk encryption for laptops is a basic step to help, as well as remote-wipe software that can be used to remove confidential or sensitive data from devices that go missing or are stolen.

6. Housekeeping

In general terms you need to make sure that only those who need access to your systems and data platforms have access, but also that you repeat these processes regularly and they are checked.

Make sure you have solid starter and leavers processes, and that you are reviewing changes and security permissions across your data and points of entry to your environment.

This is an important measure. Once these are in place the next step is easier, Audit and Review.

7. Audit and Review

Once all the good work above is done there needs to be an easy process to check it is still fit for purpose and all relevant controls are working to ensure you can see and review changes.

Most companies will have a change process in place.

If you have your own IT team or IT service provider they should be working to a framework such as ITIL v4* to ensure a review process and the relevant documentation is in place to support this with logged and authorised changes and control.

What you are looking to do with Audit and Review is to look at the changes made to the environment since the last Audit and Review and ensure the security principles still apply and that the risks those changes might pose to your environment are acceptable.

Need more support?

abbey ICT

IT • Cloud • Telecoms

We can support all aspects of your IT management, from networking, hardware and software provision, technical support, backups and, of course, cyber security. Call 01254272000 to start a free, no-obligation conversation today.