20 tips to keep your business CYBER SECURE

You should be forever looking at ways to improve the security of your firm. This guide is here to help you, your employees and your firm stay secure.

You may also be asking yourself where you spend the money to protect your firm - Many of these tips in this guide are free. In terms of spending budget on cyber security, you will always need to do this as cyber-attacks come in many forms and are becoming more frequent. It's about balancing where the biggest risks or gaps are.

We welcome any input from readers and will continually evolve this guide with new updates throughout the year.

NIKEC SOLUTIONS

1

Educate your users

Most cyber issues can be mitigated by your users. Education and ongoing training and awareness is key. This is for all your users, not just the IT team. There is technology out there that helps users, but they still need to be aware how to avoid accidental data breaches, spot phishing emails and how to improve their overall awareness on an ongoing basis.

As part of this you should have a clear policy on how your users should report a potential cyber threat, data loss or phishing email. This needs to be blame free so people own up to mistakes and the business then learns from it.

2

Multi Factor Authentifcation (MFA)

MFA is when a user's identity is confirmed using multiple credentials e.g after logging in with your login/ email you then get a code sent to your mobile or use an authentication fob or mobile app. It's secure as only the user has all the information and ensures that even if usernames/passwords are compromised, attackers will not be able to gain access with these accounts.

Be wary however and keep the MFA technology up to date as this is now becoming a common place to try and hack. Having MFA doesn't mean you won't ever be hacked, it just makes it harder for an attacker.

3

Passw****

All passwords should be changed regularly. Don't use the same password for all applications and try not to mix personal passwords with work ones. As a guide you should change passwords every 3 months and change shared passwords every time someone leaves that had access.

When choosing a password, the longer you make it - the better. Many suggest using at least 12 characters with a mix of lower and upper case, numbers, and special characters OR to use passphrases (three random words) instead of passwords!

Using a password manager for storing your passwords is also a good thing.

4

Wi-Fi

It's still surprising how many firms have open Wi-Fi. You should always protect your Wi-Fi with a password that you change regularly. Also make sure you reset the default admin Wi-Fi password at implementation, so many still leave the factory default in place.

5

Patching & software updates

Out of date software is a perfect target for attackers. Using cloud technology sometimes overcomes this issue, but keep on top of all your technology and keep auto updates on where possible.

6

Removeable Media

Limit or control the use of any removeable media such as USB devices. Not only can this cause issues if sensitive information is misplaced on a USB device, but they are also sometimes used in cyber-attacks and once you plug them in you are breached. If you are going to use a USB - make sure it's encrypted !

7

Secure File Exchange

Instead of removable media use a secure file sharing and collaboration system, such as Hubshare, to exchange any files. These systems are encrypted and will always have security controls in place.

8

Move to the Cloud

As mentioned in point 5, out of date software is a perfect target for attackers. Moving to cloud applications means you should always have the latest versions, and your vendors control this so one less thing to worry about.

One obvious solution is a cloud DMS such as NetDocuments, iManage and M-Files. They will prioritise staying up to date on the latest malware threats and deploying security patches whenever necessary. NetDocuments as an example features ransomware detection for documents that are synced to local devices. By detecting items that are being changed rapidly or when items are quarantined by local antivirus, our ransomware circuit breaker automatically disables the sync back to the platform so that any further manipulation is prevented.

9

Email

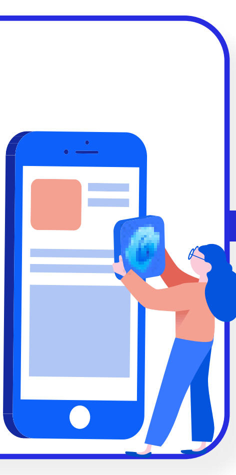
Accidental breaches are the most frequent cause of data loss in law and accounting firms. As an example, emailing the wrong person is still commonplace, and whilst you can remove the outlook auto complete, it is a pain for users and something most firms won't turn off.

We have already mentioned that exchanging documents via a secure file sharing solution is ideal and there is email software out there that prevents you emailing the wrong person also. Weaponised attachments and phishing emails are more common than ever, so having software in place, such as Tessian, to detect and protect against this is critical.

10

Secure Mobile Apps

Mobile devices are used more now than ever and can be a business's weakest link as your users work with sensitive data. There are many ways to secure mobile devices, MDM is one way and can help take the stress away from your employees worrying about encryption and security on mobile devices.



11

Minimise Apps

In general, the less applications you have the less you need to think about protecting. So, analyse the software you use and end of life any old software you aren't really using.

12

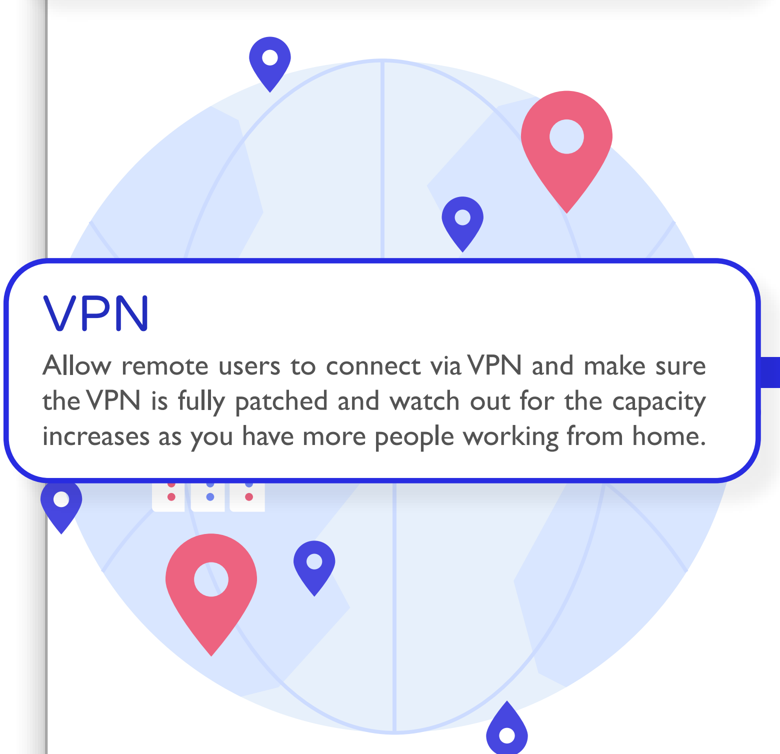
Don't use work laptops for personal use

A common issue in cyber-attacks are staff taking work laptops home and other family members then use them to play games and get breached as they download or click on something they shouldn't.

13

More than AV and firewalls

Anti-virus and anti-malware software is a must, but this is not enough to protect your firm. Invest in EDR type technology to better protect your users. (See point 16). Most firms have a firewall, but many won't have the windows software firewall turned on so check this is enabled also.



14

VPN

Allow remote users to connect via VPN and make sure the VPN is fully patched and watch out for the capacity increases as you have more people working from home.

15

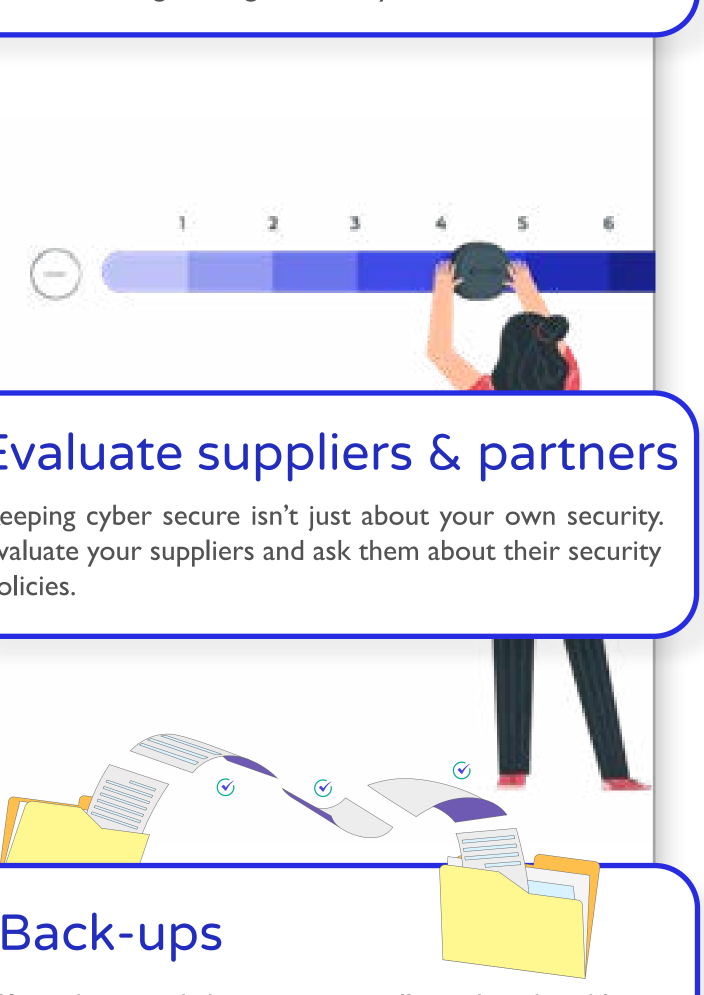
Software to monitor abnormalities

Many firms are adopting EDR solutions. If you don't have the in-house cyber teams, there are many MDR (Managed Detect & Response) offerings where they do the monitoring and leg work for you.

16

Penetration Testing

Pen testing is a proactive way to test your network or data for vulnerabilities, where they act as an attacker to try and gain access. You will then receive a report identifying areas for improvement at varying priority levels. This should be done at least once a year and make sure the vendors you use also carry out these regularly on their software, they provide to you.



17

Evaluate suppliers & partners

Keeping cyber secure isn't just about your own security. Evaluate your suppliers and ask them about their security policies.

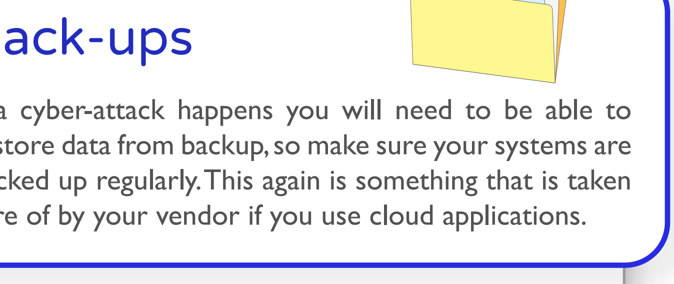
18

Certification

If you haven't already, get cyber essentials certified. This will focus the business on key things that need to be done, many of which you probably do already but aren't communicated correctly or acted upon by all users. Cyber essentials plus and then ISO27001.

CERTIFIED

CERTIFIED



19

Back-ups

If a cyber-attack happens you will need to be able to restore data from backup, so make sure your systems are backed up regularly. This again is something that is taken care of by your vendor if you use cloud applications.

20

Plan

☑ ☑ ☑ ☑ ☑

You need to plan for what to do if you get attacked. It will happen. Your software may protect it but be prepared and have a plan in place you can execute to minimise risk.

We hope this guide helps you better protect your firm. Nothing will provide 100% proof against Cyber attacks so taking action to minimise risk and protect as many areas as possible will help you stay safe and maintain a cyber secure environment.

NIKEC SOLUTIONS