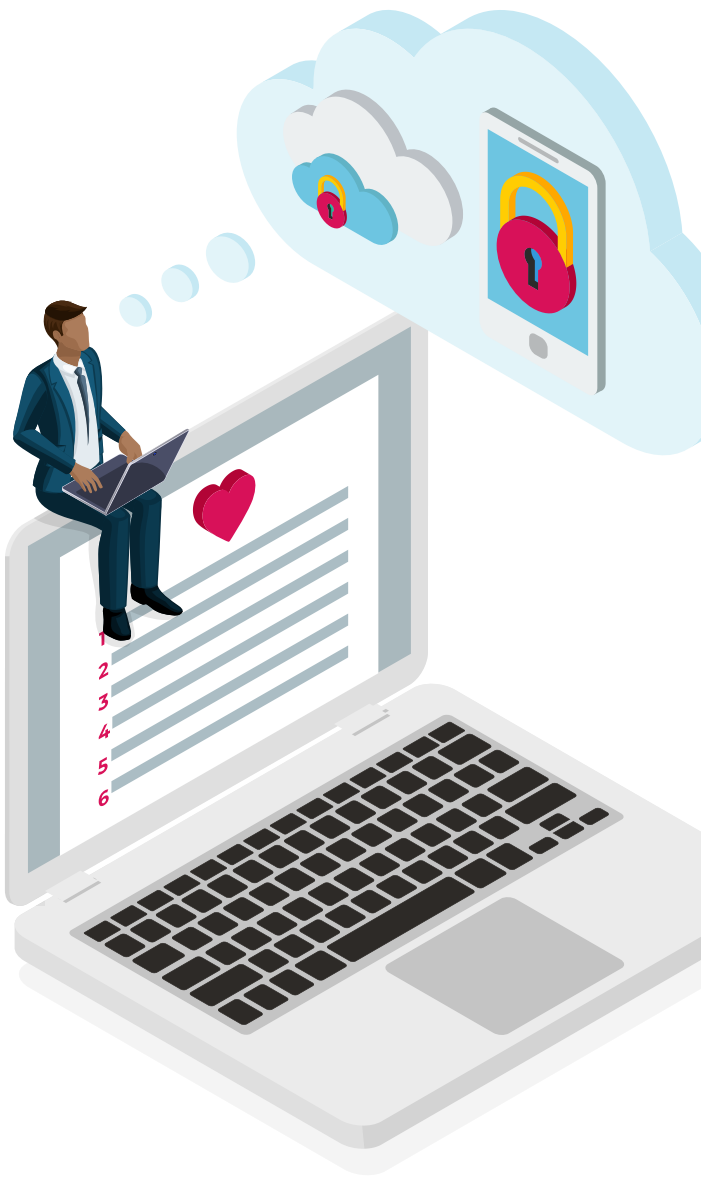
6 things cyber underwriters love



Businesses often ask what types of cyber security measures they should adopt. Here's what our underwriters and security team love to see in potential clients.

Cyber incidents are impacting businesses of all types and sizes, with cyber-related losses costing them dearly—be it through fraudulent wire transfers or ransomware attacks. But while the need for cyber insurance has never been greater cyber insurers are having to look even more carefully at each potential client to make sure they are taking adequate precautions to protect themselves.

But what are those precautions? What can businesses do to make sure they tick all the right boxes for cyber insurance providers and get the best price for their policy? Here's what it takes to get an A+.

1 Unused RDP ports are closed (and open ones are protected)

Remote Desktop Protocol (RDP) allows users to access their office desktop and computing resources remotely. While convenient, especially in the age of working from home, it can also make businesses extremely vulnerable to ransomware attacks if not configured properly. In fact, our cyber claims team estimates that over half of the ransomware attacks it deals with stem from open RDP ports, making it the single most common cause of these types of events.

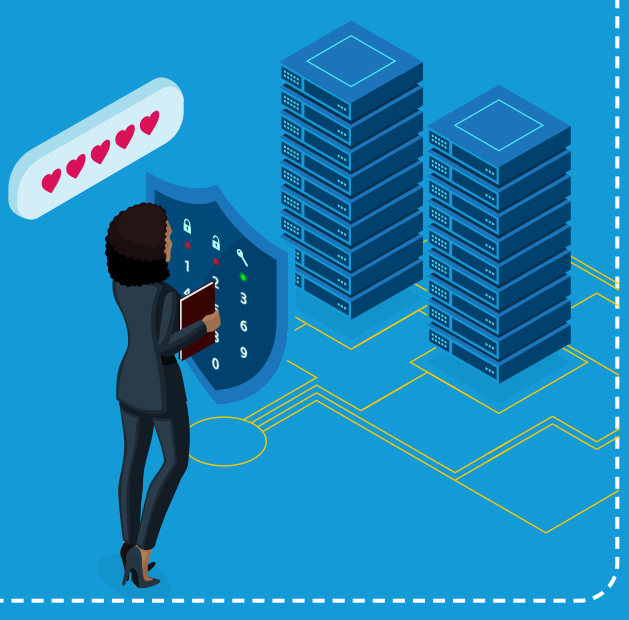
If a company's Remote Desktop Protocol is not absolutely necessary, we would expect it to be turned off. And if RDP is something that is needed, we recommend that it is secured behind a virtual private network and multi-factor authentication.

2 MFA is turned on across key business software

MFA, or multi-factor authentication, is an extra layer of security used to verify the identity of the person trying to gain access to an account. This could be anything from a thumbprint to a unique code texted to the individual.

Not having MFA in place for access to key business resources can end in disaster. Usually through brute-force attacks (where criminals try multiple username and password combinations in quick succession) or through stolen credentials from the dark web, criminals can quickly gain remote access to the organisation's network, business email accounts or clouds. This can act as a springboard for any number of cyber losses, including funds transfer fraud, privacy breaches and ransomware.

For that reason, our cyber underwriters love for businesses to have MFA in place for any remote access to their network, their email accounts or their cloud resources holding sensitive or business critical data.



3 There's a data management strategy in place

Our underwriters like to be able to quickly understand the types and amounts of data held by any company for whom they are quoting cyber cover. But more than that, they want to be able to see that the data is being stored and segregated appropriately. For example, if a business holds hundreds of thousands of client records, we'd like to see that data split across multiple servers. This means if one server is compromised, not all data is lost at once, reducing the likelihood of a business-ceasing event or catastrophic loss.

If a business outsources their data management, as many small businesses do, it's good to make sure that they have the right authorised access controls in place and that they are running security checks on any third-party partners. All of this can indicate overall good cyber hygiene.

4 Systems are running endpoint detection and response

Firewalls and antivirus software aren't enough to ward off today's more sophisticated cyber criminals. That's why our cyber underwriters love to see businesses using endpoint detection and response (EDR) tools, which continuously monitor any device that can be connected to a network – the figurative doors and windows a business has around its technology infrastructure – to ensure that each is secure and free of malicious activity. An endpoint might be anything from an employee workstation to a company server to a mobile phone.

5 Regular backups are taken using best practice

Backup practices can vary widely, so our cyber underwriters would like to know more. How often are they taken? Where are they stored? Are they backed up regularly and separated from the live environment, either with offline back-ups or with cloud back-ups secured by MFA. After all, out-of-date backups or backups that are kept on the same system as the files they are backing up aren't much use when the whole system is compromised.

Having good backups can be the difference between recovering systems relatively quickly and easily following a ransomware attack and forking over a six or even seven figure extortion demand to criminals that have encrypted entire systems including backups.

6 Applying updates and patches for vulnerabilities in a timely manner

Keeping your computer systems up to date with the latest fixes and patches helps to protect sensitive data and prevent cyber attacks. Whether you're advised by CFC or by the relevant platform it self, by staying ahead of these threats you can retain and build customer trust, while avoiding financial losses. It's like locking your doors to keep burglars out.

Our cyber underwriters love to see a willingness to implement fixes for security vulnerabilities that our in-house security team has detected and to use our cyber security services – specifically our mobile app – to educate employees and detect vulnerabilities.

CFC have your back when it comes to safeguarding your business.

From the moment a CFC cyber policy is bound, we work around the clock to protect that business against cyber attacks. Using insights from threat intelligence feeds, the dark web, network scanning and our own real-life claims data, we identify potential threats and alert vulnerable customers before the worst happens.

If our monitoring or intel feeds alert us to a business being at risk, we'll reach out through our mobile app with a critical threat alert and offer assistance to prevent the any attack from occurring.

Want to learn more? Visit cfc.com/cyber