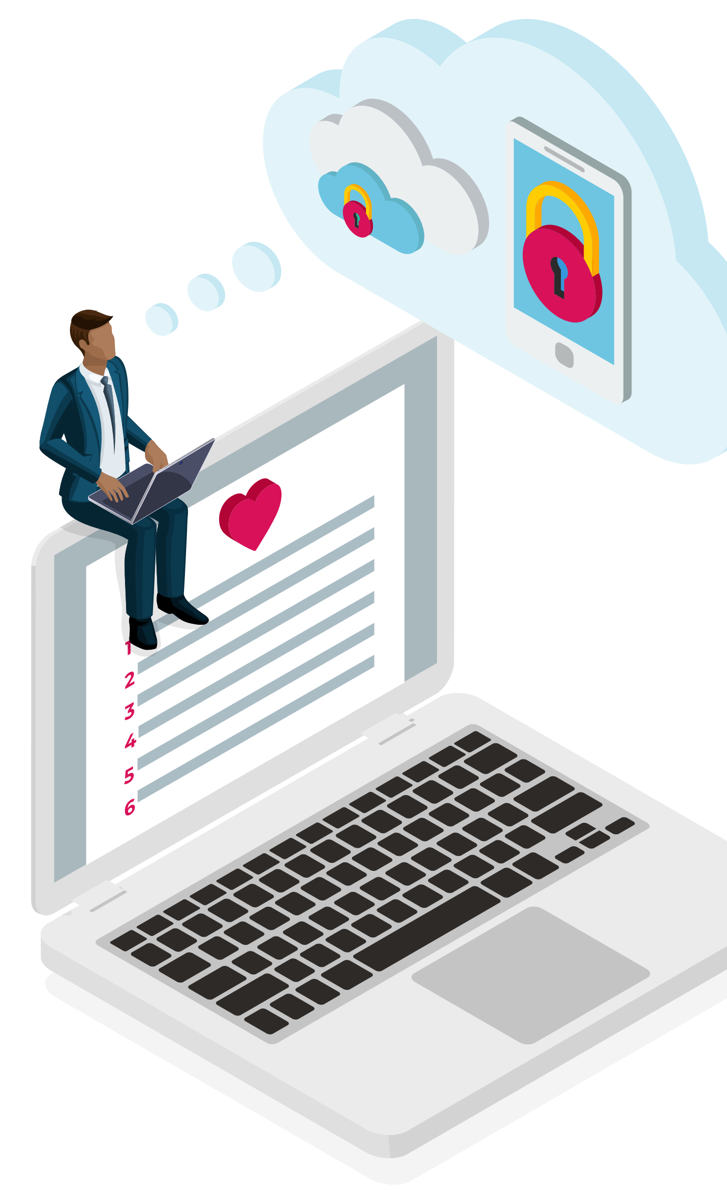
6 things cyber underwriters love



Clients often ask what types of cybersecurity measures they should adopt as a business, so we've spoken to our underwriters and security team at CFC to see what they love in potential clients.

If one thing's for certain, it's that cyber incidents are happening to businesses of all types sizes and it's costing them dearly. Businesses are getting stung by cyber-related losses like fraudulent wire transfers and ransomware attacks more than ever. This has meant that 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 the most basic precautions to protect themselves.

But what are those precautions? What can businesses do to make sure they are ticking all the right boxes for cyber insurance providers and getting the best price for their policy? Here's how clients can get an A+ in our view:

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.

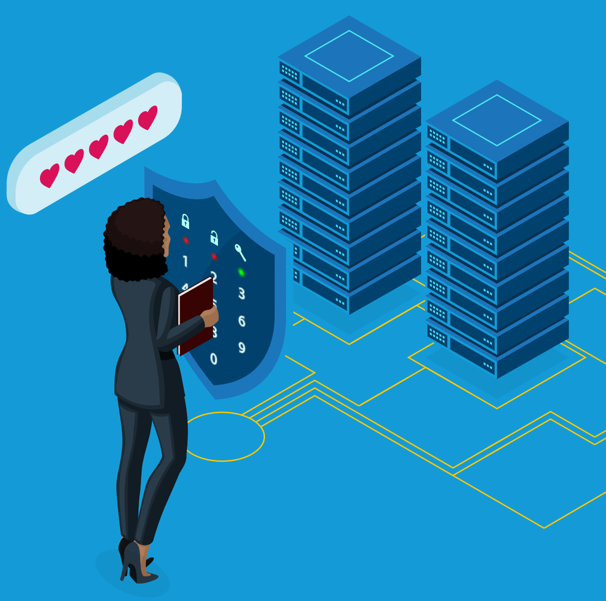
If a company's Remote Desktop Protocol is not absolutely necessary, we would expect it to be turned off. And if RDP is something that is needed, we recommend that it is secured behind a virtual private network and multi-factor authentication.

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 and is a nearly ubiquitous feature across technology platforms these days.

A lack of MFA on business email accounts or RDP can be a 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 (as so many people reuse username and password combinations), criminals can quickly gain access to business email accounts without this extra piece of security. This often results in funds transfer fraud losses where money is rerouted to fraudulent bank accounts, but it is also increasingly leading to ransomware events and major privacy breaches.

For that reason, our cyber underwriters love when a business has MFA in use across all business email accounts and on other key business software too.



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 100,000 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 cybercriminals. 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? We are keen to see that data is being backed up regularly, segregated from the main network, and stored offline in an offsite location. Afterall, 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 in 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 A good attitude towards risk management is demonstrated

Often times, our underwriters simply want to see evidence that a business has good security governance. Does a business have policies and procedures in place in relation to cyber risk management? Have they put a person in charge of these policies and procedures? Are they aware of the different kinds of data they hold and how it's stored?

A willingness to implement fixes for security vulnerabilities that our in-house security team has detected and to use our risk management services – specifically our mobile app – to educate employees and detect vulnerabilities also demonstrates a lot about a business.

CFC's in-house cyber security team does a lot more than respond to events after the fact.

In fact, more and more of what we do is to work with clients to identify where holes in their security posture might be, and then support them in remediating any vulnerabilities and strengthening their overall security.

This might happen when we quote the risk, when we notice a particular claims trend emerging about a specific type of business, or through the vulnerability monitoring provided by our mobile app.

Want to learn more? Visit our cyber product page.