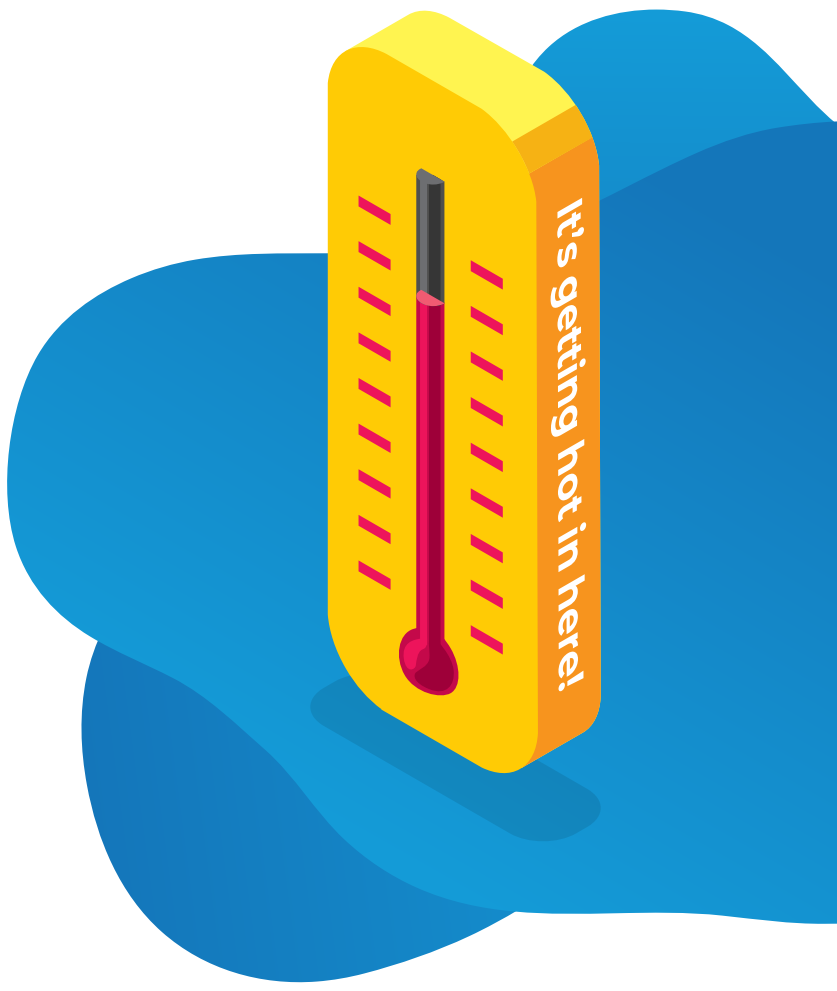
Cyber risk heat map



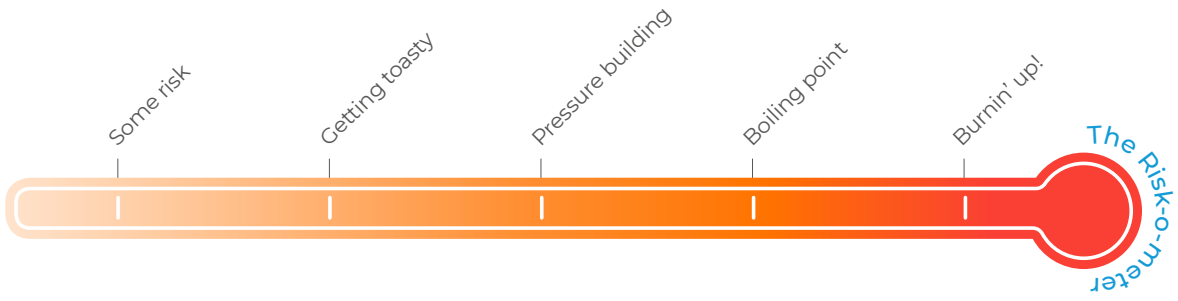
For brokers wanting to start a conversation about cyber insurance with their clients, it's important to focus on areas that are truly relevant to the industry they operate in.

Our cyber risk heat map was built from data relating to the thousands of cyber claims we've dealt with in the last few years, as well as trends that our incident response team is witnessing. This color-coded graph ranks the severity of different industries' exposure to business interruption, privacy, and cybercrime and include examples of how these exposures can play out for different types of organizations.

Not sure where to start?

Follow these three easy steps:

1. Find the sector
2. Find the exposure
3. See where this intersection lands on the Risk-o-meter – we've included a few scenarios specific to the sector



Industry

Exposure	Construction	Education	Healthcare	Manufacturers	Professional service firms	Public entities	Retail	Technology	Transport/logistics
Business interruption & system downtime	The system of one of your major suppliers goes down, creating a knock-on effect as you're unable to get the materials you need in time or at the same price	Key resources, including student data, lesson plans and educational materials, are rendered inaccessible by a ransomware attack	A cyber event disrupts operations resulting in cancelled appointments, staff overtime and rerouted services	Production slows or stops due to problems on your own system or on the systems of your supply chain partners	A customer database is corrupted as a result of malware attack, requiring the data to be re-created from scratch using paper records	Public services come to a halt after a ransomware attack locks down systems and prevents access to key operational information	Your business loses revenue, and customer loyalty, from an inability to operate in-store or online due to a cyber attack or system downtime	An application bug causes system downtime and impairs your tech services, resulting in customers taking their business elsewhere	A ransomware attack prevents you from using your tracking systems leading to large delays, lost items and staff overtime costs
Privacy	Sensitive employee data, including social security numbers and health information, is accessed by hackers and posted on the dark web	Hackers manage to access personal information, including student health information, and you must notify all parents of the breach	PHI is lost or stolen leading to widespread notification, corrective action plans and other regulatory expenses	Hackers steal commercially sensitive information, including product designs and blueprints, and threaten to publish them online unless a ransom is paid	A spreadsheet is accidentally sent to the wrong email address containing confidential information, requiring notification to be sent to all affected	Sensitive information about residents, including names, addresses, birth dates, income status and political party is stolen from you and posted on the dark web	Your customers' credit card information is stolen and you must pay the costs of notifying, as well as regulatory fines and penalties	Client data that you're responsible for protecting gets stolen, and you're held liable	A rogue employee sells sensitive data on employees and customers on the dark web, resulting in notification costs and reputational damage
Crime	You pay a large, seemingly-authentic invoice to a supplier, only to realize that it was a fake and the money is now irretrievable	A phishing campaign results in compromised employee email accounts which hackers use to reroute tuition payments	A payment intended for a medical supplier is intercepted by cybercriminals via a social engineering attack	Cybercriminals fraudulently intercept wire transfer payments made between you and your supply chain partners	Hackers gain access to your business email and reroute your clients' invoice payments to fraudulent accounts	A payment for a construction project is redirected to a fruadulent account by cybercriminals who have manipulated an invoice payment	Fraudsters set up a fake website impersonating your store and sell fake items, resulting in you reimbursing affected customers for their loss	Cybercriminals exploit your computer resources for cryptomining, resulting in increased electricity costs and cloud service billing for your business	Your online banking account is compromised by hackers, resulting in numerous transfers to fraudulent accounts

Did you know?

Ransomware accounted for 71% of cyber claims costs we faced in 2023.

CFC Cyber Claims, January – December 2023

No matter your industry, you can still be at risk to a **ransomware attack**

Use our calculator to understand how much a ransomware attack could cost a business.

You'll be sent a custom report which provides:

- A ransomware severity loss estimate
- Actionable tips to prevent ransomware attacks

Calculate the cost now!

Learn more about CFC's market-leading proactive cyber offering at cfc.com/cyber