Cyber risk heat map

Built from data relating to 2,500 cyber claims

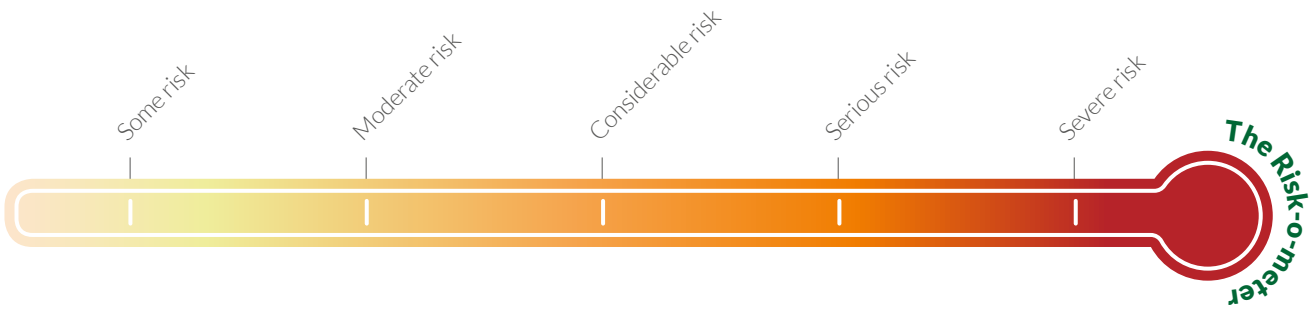
Cyber insurance has a long reputation as a privacy liability product for businesses that hold sensitive data – but privacy exposure isn't the only risk facing businesses today. In fact, cybercriminals are increasingly targeting traditional industries that hold almost no sensitive data at all, whether through ransomware attacks that halt operations or business email compromise scams that result in wiring payments to fraudulent accounts.

Many companies find themselves confused about how cyber insurance actually works. It is important to focus on the areas that are truly relevant to the industry you operate in.

The below cyber risk heat map was built from data relating to 2,500 cyber claims from the last two years as well as external cyber security threats. This color-coded graph ranks the severity of different industries' exposure to business interruption, privacy, and cybercrime and includes a few examples of how these exposures can play out for different types of organisations.

Not sure where to start? Follow these three easy steps:

1. Find the industry
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

Exposure	Construction	Education	Healthcare	Manufacturers	Professional service firms	Public entities	Retail	Technology	Transport/logistics
Business interruption	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		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		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		A ransomware attack prevents you from using your tracking systems leading to large delays, lost items and staff overtime costs
Privacy		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			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	
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		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				

This heat map was produced by cyber insurance specialist, CFC. For more information about CFC, visit www.cfcunderwriting.com or speak to your Partners& insurance broker.