



Five reasons hackers target SMEs



While the massive influx of remote working has alerted many businesses to the risk of a cyber attack, it has also created more opportunities for cybercriminals to take advantage of this new way of working.

Cyber claims rates are on the rise. The majority of victims being hit by cyber crime are small and medium-sized businesses, and include funds transfer fraud, and ransomware attack.

We spoke to CFC Underwriting ([CFC](#)) who outlined the five reasons these organisations appeal to cyber criminals.

1 Small businesses are low-hanging fruit

While the headlines focus on major security breaches at major companies, small and medium sized businesses are actually the more common victims of cyber attacks. In fact, the Federation for Small Businesses (FSB) estimates that small firms are being hit with upwards of 10,000 attacks daily¹ Even though the rewards may be less, cybercriminals see smaller organisations as low-hanging fruit because – due lack of education and resources – they usually invest less in IT security and don't often train their staff on cybersecurity risks.

2 Small businesses are more vulnerable to social engineering

Social engineering is an act of manipulating people into doing things like share confidential information or wire money. Small businesses tend to be more exposed to this risk for a number of reasons: they have less basic security in place, like two-factor authentication; they don't often know the risk or train employees; they usually work with a variety of third-party partners to run their business which is the root cause of 41% of data breaches²; and they almost always makes and receive payments using wire transfers.

3 Small businesses often feel they must pay ransoms

Faced with choosing between paying a ransomware demand that may get them back online faster or enduring a long period of potentially business-crippling downtime, small businesses often feel that they have no choice but to pay these demands in the event of an attack. Without anyone to turn to for help, this is particularly true of those without access to the cyber incident specialists that cyber insurance can provide.

4 Small businesses are the 'gateway' to larger organisations

Many SMEs are connected electronically to the IT systems of a range of larger, partner organisations. So when cybercriminals are looking to infiltrate these larger and more cybersecure organisations, they are increasingly targeting their humble downstream suppliers to see if these small businesses offer a less secure way in. What's more, many of these IT relationships are visible through publicly available data.

5 Small businesses are sometimes not targeted at all, but simply collateral damage

From the WannaCry attack of 2017 to the Kaseya Incident more recently (the biggest global ransomware attack on record), SMEs are often collateral damage in large-scale cyber attacks that have nothing to do with them. Small businesses might think they are safe because they outsource their IT and their data is stored in the cloud, but if a cyber attack is launched against one of these technology providers, it's the businesses that rely on it that are often left footing the bill, whether paying for the business interruption costs involved, privacy notifications to customers, or reputational harm.

A cyber crime incident can be devastating to your business. We work with a number of insurers such as CFC to offer organisations the right cyber insurance policy to protect them. If you would like to discuss the ways we can help protect you against such a risk, please contact your local branch of **PIB Insurance Brokers** or your usual contact.

Sources

¹ <https://www.fsb.org.uk/resources-page/small-firms-suffer-close-to-10-000-cyber-attacks-daily.html>

² <https://www.cfcunderwriting.com/en-gb/>