Smash and grab

James Brady warns that SMEs are big business for cyber criminals and it is important to guard against cyberattacks.

TEN SECOND SUMMARY

1. **Although it is cyberattacks on big business that receive national publicity, this does not mean that small businesses will not be victims.**
2. **A cyber breach can be costly with ransoms being paid, hardware and software having to be replaced and charges for expert advice.**
3. **Businesses must remember that the General Data Protection Regulation requires organisations to have measures in place to protect data.**

James Brady is Head of Cyber, Hiscox UK & Ireland and leads the Cyber and Data Insurance division of Hiscox in the UK and Ireland.
Visit: tinyurl.com/Hiscox-cyber

The thought that "It'll never happen to me" is a common misconception that most of us have hidden behind at some point or other – often when faced with a potentially daunting or unpleasant possibility. In the context under discussion here, that possibility is being the victim of a cyberattack, and it's UK small businesses that are doing the hiding.

It is rare that a day passes without there being a story in the press about another organisation brought to its knees by cyber criminals. The attack on British Airways for instance, was barely out of the headlines before the next attack on Cathay Pacific – said to be the world's biggest airline data breach – was reported. The scale and severity of these attacks warrants attention from the media, but also creates a dangerous perception gap and fuels the widely held belief among small businesses that they are too small to catch the attention of cyber criminals or that bigger, higher profile organisations are the more likely targets.

The prolific targeting of SMEs

In the UK, a small business suffers a cyber breach every 19 seconds. To put that into context, that's around one in every three small businesses being attacked each year. To make matters worse, the firms being targeted are often the victims of multiple attacks – and about half of these organisations go on to suffer multiple breaches. This leaves those businesses with a hefty bill for picking up the pieces.

The direct cost of a cyber breach is easy to quantify: the ransoms paid, the cost of replacing hardware and software, the bill for expert advice, to name but a few. On average, these outgoings add up to about £25,700 a year for a small firm that suffers a breach, but it's the indirect costs such as damage to reputation and loss of future customers that are harder to quantify. Often, these expenses can be the final straw for a struggling small business.

Source of cyber breaches

Without doubt, cyber criminals are becoming increasingly sophisticated. Attacks are becoming more complex and the scale more significant, but old habits die hard and there are some more common types of attacks that keep catching out businesses.

Hiscox dealt with more than 1,000 cyber-related claims in the past year. Ransomware, which puts a business's computer system out of action until a ransom is paid to the hacker, is our biggest source of claims. This type of breach was made famous by the Wannacry and Petya attacks in 2017, but this cyber weapon is equally as effective on a smaller scale, perhaps due to the low barrier to entry for hackers, ease of deployment and the prospect of a decent return on a minimal investment.

Recently we have seen many claims which begin with criminals hacking into customers' email accounts. Personal and confidential information was accessed, with emails often being sent from the hacked account, frequently asking for payments to a bogus bank account. This is also known as payment diversion fraud.

Although a considerable proportion of cyber breaches are the result of a malicious, external "attack", an alarming amount stem from internal "accidents" in which data is lost or misused. An employee leaving a mobile phone on a train is a good example – although innocent in nature, the impact can be equally as catastrophic.

Prevention

In effect, the astonishing regularity of cyberattacks on small businesses is down to two intrinsically linked issues: the increasing sophistication of cyber criminals and the inability – or in some cases unwillingness – of small businesses to build a robust defence. This is not to say that firms aren't getting better at prevention, because they are, but this rate of improvement is slow in comparison with the progress made by criminals.

The fight small businesses have on their hands is epic, but a recent study confirmed the shocking extent of this. As part of a broader awareness campaign, we set up three "honeypot" computer systems, typical of those used by small firms across the country and monitored the number of attempted cyberattacks. The total number ranged from 900 to 359,000 each day, averaging 65,000 over the course of a few weeks. Faced with those figures, it seems counter-intuitive that the steps small businesses can take to defend themselves are relatively straight-forward, but it's true. Good cyber security doesn't have to be that complicated, or even costly.

Small steps, big impact

Instituting cyber training during the onboarding process and keeping this updated is one of the most effective prevention techniques – think of it as building a human firewall. Around two-thirds of all breaches result from some form of employee error because this is an easy entry point for cyber criminals, but this is completely unnecessary. Involving and educating people at every level of the businesses is key – a strategy that's confined to the boardroom, or conversely the shop floor, is of limited use.

However, prevention alone is not enough and having a plan in place to deal with an attack if and when it occurs and one that covers people, processes and technology is crucial. Much like a fire alarm, this needs to be tested regularly to ensure it works, and that people respond in the right way. Simulating an attack or conducting a phishing experiment will tell a firm how prepared it really is and will help keep employees engaged and on their toes.

Is insurance necessary?

A common misconception about cyber insurance is that it exists purely to cover the financial costs of a breach. Although this is a fundamental part, a good policy should provide access to a network of experts who will help manage an attack and mitigate against further damage. This can provide practical support in the time-sensitive moments when an attack is happening, drawing on the expertise of forensic investigators, PR consultants, legal advisors, credit monitoring agencies – in essence, an "A-team" of cyber security support. While less common, some insurers may also offer support with employee training. Ensuring that small business customers without in-house expertise have a knowledgeable workforce in this area is important. This is particularly valuable to small businesses since the introduction of the General Data Protection Regulation (GDPR) earlier this year. This requires organisations to implement "appropriate technical and organisational measures" to protect the data that they hold and process.

Don't be the "one" in "one in three"

The misconception that small businesses aren't worthy targets for cyber criminals is a costly perception gap. For a small business, there's a one in three chance that it *will* happen to them but there's plenty that can be done to avoid it and limit the impact when it does happen. Good cyber security takes time and investment, but the resource and money required to stop or limit the effects of an attack are, thankfully, relatively slim in comparison.

FURTHER INFORMATION

The Hiscox CyberClear Academy is a government-certified cyber security training platform, which has been widely used by small business customers who don't have the in-house expertise or time to up-skill their workforce. Small businesses should not forget that the General Data Protection Regulation requires organisations to implement "appropriate technical and organisational measures" to protect the data they hold and process. Visit: tinyurl.com/Hiscox-cyber