Blackford.

No PICNIC

How to stop cyber scammers eating you for lunch

01 September 2023

Ready for Anything.

One of the worst things about going on a picnic is the panoply of devilish critters which gatecrash the occasion and want to share your lunch. Pop open the sandwiches and pork pies, and you can all but guarantee that, minutes later, you'll be swatting away squadrons of wasps, flies, and all kinds of unidentifiable winged pests.

There's usually a point at which something particularly revolting, like a greasy, corpulent bluebottle, lands on your chicken drumstick and renders it inedible. Not only is it infuriating, but it's a bit of a spanner in the works for the whole picnic.

Now imagine the flying pests are cyber hackers, and your meticulously-prepared packed lunch is your company's IT infrastructure. A fly in the cherry tomatoes tends to disrupt your lunch plans (even if no-one ever eats the salad).

Insuring your tech set-up is a simple enough thing to do in itself. Talk to your favourite broker, work through the insurer proposal forms, and off you go. But there's a critical step which most people miss and without which insurers won't go near your business.

The most important part of cyber insurance? A proper cyber strategy.

The weakest link

Now it's time for a different type of picnic – a PICNIC. The insurance and tech sectors share a love of jargon and acronyms, and this one is especially enjoyable. When it comes to diagnosing what goes wrong for most companies' cyber defences, the Problem is In the Chair, Not In the Computer. PICNIC.

That memorable – if slightly contrived – mnemonic addresses a key point in cyber defence. Your defences are only as good as the people who use it. **Hackers rely on a second's inattention, a gap in the knowledge, an uncharacteristic second of gullibility.** One slip and they're in. And that's what you're up against.

To combat the issue, as we're sure you're aware, it's important to put in place a thorough cyber defence plan. Once it's in place, it has to be a living, breathing thing which becomes an intrinsic part of how your business grows and operates.

We spoke to Alana Muir, head of cyber at insurer Hiscox, to find out more about what insurers look for when it comes to cyber cover – and how companies can limit the chances they'll need cyber insurance in the first place.

WHAT IS CYBER INSURANCE?

Most insurance products focus on restoring something to its original or a comparable state if something goes wrong. Rebuilding after a fire or flood, replacing or repairing a vehicle, or in some cases providing financial compensation if things don't go to plan.

Cyber insurance is a bit different. As Alana said,

"Cyber insurance is more of a service. Whether it's a data breach or a cyber attack, you've got somebody in your corner."

In a 'cyber event' – shorthand for some kind of breach, attack or other mishap – most insurance products will provide you with a triage service to help you deal with what's going to be a pretty stressful situation. You might be working with a 'breach coach' to coordinate the various moving parts, making sure you get the right advice and input from IT forensics experts to confirm what's going on and how to deal with it; legal advisors who can make sure you stay on the right side of data protection laws; and PR specialists to help defend your company reputation across key communications channels.

If the data regulator – the Information Commissioner's Office (ICO) in the UK – decides to conduct a further investigation once you've notified it of a data breach, your cyber policy should also cover the cost of this.

Why is this important?

In most businesses, financial considerations are priority number one, and operational considerations are a very close second. All very fair and appropriate, but in many companies you have to look quite far down that list of priorities to find 'cyber security'. Sometimes it's a footnote on board risk registers, or it's siloed in the IT department and paid lip service when it comes to practical implementation.

We've all read news stories of companies suffering large-scale data breaches over the years. When it's happening to FTSE100 companies it can feel a bit distant, and it's tempting to think the big players are more attractive targets than SMEs based in the UK and quietly going about their business.

However, in the most recent global research from Hiscox, highlighted in its 2022 Cyber Readiness report, 48% of companies have already experienced at least one attack. IBM reported in summer 2023 that the average data breach now costs £3.5m. For companies which had deployed extensive security artificial intelligence and automation, that average drops to £1.6m. It's a chunky discount for deploying the right technology, but still leaves a serious cost to deal with.

Despite this, the researchers found that organisations which have experienced a breach (and 95% had experienced more than one) were more likely to pass the costs onto clients and customers than to invest more in security.

Don't assume these are all huge organisations, either. The research looked at breaches between 2,200 and 102,000 records, which could comfortably include plenty of SMEs.

Ultimately, however, cyber events cost money, and the costs are increasing. Depending on the scale and severity, it could be a nuisance or it could be a major threat to the business. There's the direct cost of lost business and downtime, as well as potential reputational impact and the cost of improvements which weren't previously factored in. At the very least it's a drag on profitability.

What we're saying, and we're assuming that most people now get this quite clearly, is that cyber security can't be a peripheral issue. It has to be an intrinsic part of how your business operates every day.

How hackers find their way in

As you'll no doubt have heard said before, cyber attackers are clever, capable, well-resourced and extremely determined. But it's probably not quite correct to imagine a cackling youth tapping feverishly away on a keyboard in a dingy basement (although we're sure this still goes on). The more realistic scenario is a phalanx of automated bots crawling servers, looking for any number of weak spots to exploit; simultaneously unleashed on thousands of businesses all over the world.

It won't be any comfort to hear that it's unlikely you've been specifically targeted. What tends to happen is more of a 'spray and pray' effect, where the sheer volume of targets usually yields results for the attackers.

That could be the result of a weakness in cyber defences or operating systems which allows them to lob in a virus and let it work its dastardly magic. Or it could be an email phishing scam, whereby someone unwittingly clicks on a link, unleashing ransomware which brings the whole system to a halt.

According to Alana from Hiscox, the Ukraine-Russian conflict has resulted in military-grade hackers opting for new career paths in the private sector. These individuals have the experience and skills to circumvent the security systems of national governments and their various agencies. Their emergence as cyber guns-for-hire working for the highest bidder is another, terrifying reason to tighten up your defences.

There's also the possibility that hackers won't find their way directly into your network at all. It's likely that at least some of your data is stored remotely in the cloud – either with one of the large hyper-scalers like AWS or Microsoft Azure, or a private cloud managed service provider (MSP). Cyber criminals know this and can direct some of their efforts towards breaching a cloud network, potentially giving them access to thousands of organisations in one fell swoop.

We should point out, of course, that cloud providers usually have some of the most robust defences on the market and in no way are they a soft target. But the fact remains that no-one is infallible and your security is your responsibility, even if you host your data externally. If your MSP suffers a breach, your security set-up shouldn't be like an open door for attackers.

As Alana points out:

"Outsourcing your IT does not outsource your responsibility for the data."

Get cyber insurance ready

Cyber insurance clearly takes a bit more up-front effort than what might be considered more 'traditional' insurance policies. But the principle is the same – insurers want to see that you've taken reasonable steps to prevent a problem arising in the first place.

If you were insuring yourself against property damage you'd avoid building your new factory on a known flood plain, for example. Similarly, if you want to persuade insurers you're a safe bet in the modern online world, you'll want to put in place some sensible measures to reduce your risk.

It's not just about specific IT security measures however. As we mentioned at the start of this paper, cyber problems quite often arise through human error rather than porous IT infrastructure.

Insurers will also look at your people management and the overall governance of the organisation when it comes IT security. For example, how good is cyber security training and how regularly is knowledge shared and updated across the business? Treating cyber security as a one-off event could signal to insurers that it's not being taken seriously or, worse, that it isn't properly understood.

Insurers are always hoping to see companies that have taken the time to understand and articulate their specific risk exposure. For example, are you most at risk from business interruption from a denial-of-service attack, where your network is effectively crippled by a constant barrage of data? Or if you're a manufacturer, is your vulnerability more around your systems dependency; or a medtech company with responsibility for extremely sensitive customer data?

Businesses should be able to show prospective insurers an awareness of their risks and how seriously these are viewed. Ideally they'll be a board level issue and not pushed down the chain without the correct level of strategic oversight.

Many insurers themselves now offer internal training for your staff as part of their efforts to reduce their own risks. This applies to senior leadership as much as – if not more than – other staff, since C-suite staff are sometimes less directly involved in cyber issues and can unwittingly open the doors to what IT experts call 'bad actors'.

The SME with a £5 million loss

A lot of SMEs assume that because they operate on a relatively small scale their financial risk from cyber attack is proportionally moderate. But it's not always the case and losses can accumulate at a frightening rate.

We asked Alana from Hiscox if smaller companies are safe to assume they're at lower risk. It feels like a reasonable position to take when most of the breaches we read about affect companies with millions of customer records and huge operations across the world. Her response was an eye opener:

"I have a client that has 17,000 records, which wouldn't be considered a lot of records. It's a UK firm but they do have some overseas customers.

"They suffered a £5 million loss in a recent breach they've had.

"You wouldn't have expected that but it's because the client base is multinational. Even if you're an SME and you operate solely in the UK, but you have customers around the world, you have to adhere to that data protection legislation in each different country.

"In the US, for example, each State handles it completely differently. You can see how you would need the support of a solicitor in the State with an understanding of the legislation."

SECTOR FOCUS – MANUFACTURING

Manufacturing is often seen as a bellwether for the rest of the economy, with the principle of 'making stuff' usually associated with a country in rude financial health. Today's manufacturing businesses have as much in common with tech firms as high-value, precision manufacturing has grown in response to global competition and productivity demands.

This creates vulnerabilities, however, and Alana from Hiscox said that manufacturing firms are particularly at risk from hackers.

Before, operational technology tended to work offline – any computer systems were limited to the local network on which they operated. As technology has advanced, and skills have become ever-more in demand, the constant need for greater efficiency brought manufacturing firms into the world of internet of things to control and co-ordinate production lines.

Unfortunately, IT security hasn't always been sufficiently integrated into operational technology, meaning a single impact on the production line could take down the entire business.

As is so often the case, the cultural legacy of many manufacturing businesses means these kind of issues can be a blind spot. The reality is that upgrading IT security for manufacturers can also be a substantial investment.

Separating IT and operational technology to allow isolation in the event of an attack is an important priority for manufacturers. That way, even if the internal network is breached, it's possible to stop attackers reaching the production line and causing even more chaos.

SHOULD YOU PAY A CYBER RANSOM?

Some cyber hackers will lock a business out of its own network and demand a ransom payment to restore access. Should you pay and will insurance cover it?

The average ransom demand is £500,000, to which can be added the average recovery costs of £1.3m, according to Sophos, the cyber security firm. It might be tempting to pay a ransom to get your business back up and running again but a) there's no guarantee the hackers will reinstate your systems and data (Criminals? Dishonest? Really?) and b) you'll probably be added to a 'sucker' list, ie you stand a good chance of a return visit from your unwanted guests.

In some countries (not the UK) it's actually illegal to pay ransom. The UK government position is currently that it doesn't want companies to suffer a cyber-attack then face criminal sanctions for paying ransom to get their business operational again, but that approach may change. A cyber insurance policy can cover ransom payments where legal and appropriate, but in general insurers don't want to pay ransoms for the simple fact that these payments can be used to fund financial crime, terrorism and other criminal behaviour. We've seen examples where criminals have targeted organisations known to carry cyber insurance and frame their ransom demand as a victimless crime where the policy cover is viewed as 'free money' with no cost or harm to the targeted business. Insurers monitor this issue very carefully and will check into the source of ransom demands to make sure they don't fund known criminal networks, and whether the source has a track record of releasing the data as promised. In short, it depends. No-one wants to pay criminals, but where such payments are legal and where there's no other option, it does happen.

Ready for a connected world

Cyber crime is as much a reality of modern life as fire, theft and fraud. Technology has created a connected world which allows us to communicate and trade with other businesses all over the world without having to leave our offices or homes.

For ambitious businesses looking for growth, that's a mightily exciting prospect. But every opportunity carries risk and, unfortunately, there are criminals in every walk of life who'll find a way to exploit weaknesses.

That doesn't mean we should scale back our ambitions – with the right planning and thought you can make your business a less attractive prospect.

There's an old joke where two big game hunters are confronted with an angry lion. One hunter starts pulling on a pair of running shoes, at which his companion scoffs: "Trainers won't help you outrun a lion." The first hunter replies: "That's OK, I just need to outrun you."

You need to make sure you're not the easy meat.

Insurers don't expect you to discover the secret of cyber invulnerability, but they are looking for a considered approach which covers technology, people and governance.

Cyber insurance can be an effective way of getting your business back on its feet if things do go badly. There's practical, expert help in place to make sure you can tackle the regulatory, legal and other issues that can result from a cyber breach, not to mention expert support to lean on in a difficult situation.

Insurance can't stop hackers any more than it can stop fire and flood, but we all know that you can do everything right and things will still go wrong.

We loved this last word from Alana at Hiscox:

"The pandemic taught us that we could trade without our physical assets like property. That's a very valuable asset. That's something we insure as standard.

"But why would you insure the asset you can trade without, and not the one you can't – your data and your systems?"

For the full interview with Alana Muir from Hiscox, visit www.blackfordinsurance.com