Cyber security risks for small businesses

November 14th, 2019

Data and tech

Share article

Stephen Ridley

Stephen Ridley is Lead Cyber Underwriter and Product Head for cyber and data risks at Hiscox UK and Ireland.

Meet our authors

Share article

Staying ahead of cybercrime

This year we conducted our third annual **Cyber Readiness Report**. It's an up-to-the-minute picture of cyber readiness in organisations of all sizes, as well as a guide to best practice against the ever-changing threat of cybercrime.

It's a mixed picture – we've seen progress in some areas, with regulation helping to improve awareness, most notably the 2018 introduction of the EU's General Data Protection Regulation (GDPR). We've also launched our own online training platform, the CyberClear Academy, to better equip customers and already more than 2,500 companies have benefited from it.

More firms are taking a structured approach with a defined role for managing cyber strategy, but cybercrime demands constant vigilance – it's a constantly evolving field. Larger firms are still most likely to be hit, but the proportion of small firms reporting one or more incidents is up from 33% last year to 47%. With an increasing proportion of smaller firms caught up, let's refresh ourselves on why protection against cybercrime matters and how you can stay one step ahead.

Small businesses and cyber threats

In last year's report we looked at more than 4,000 organisations across the UK, US, Germany, Spain and the Netherlands and found major shortcomings in readiness at 73% of firms. For small to medium-sized UK businesses of under 250 employees, the failure rate was higher, at 78%.

Of those smaller businesses hit by an attack, more than half were compromised twice or more in the same 12-month period. We already know from our research in 2017 that **small businesses take longer to recover from cyber attacks** – even a day's disruption can have a significant impact. But it's not just about the frequency of attacks, or even the difficulty in getting back to normal, it's about building a broader awareness too. Small businesses play a crucial part in many major cybercrime plots, they're easier to hack than big corporations and they're often connected to larger supply chains. It's not just your own business, data and reputation at stake, it's those you work with too.

For example, anyone acting as a supplier to trains, buses, planes, energy companies or any other organisation considered critical to the national infrastructure could provide a back door for hackers. Four of the biggest hacks in the world to date – Sony, AT&T, eBay and Target – were possible because of a third-party supplier being compromised. If enough small businesses were attacked it could even threaten a country's financial infrastructure.

Cyber threats are always changing

As the world becomes more hyper-connected, the cyber security risk increases every day. The types of threat are changing as fast as the technology. Businesses are increasingly relying on cloud computing, which creates a single point of cyber security failure. There's a narrow, precarious path between harnessing technology to give a competitive edge and staying mindful of increased security risks. If you decide as a business to hold more data to improve your services or to move to a cloud environment then you need to make sure you have appropriate security measures in place.

The explosion in the Internet of Things is another flashpoint and the inventiveness of hackers knows neither mercy nor bounds. The **Mirai botnet** for instance, took over an army of webcams and modems that disabled vast tracts of the internet. More recently, it was discovered that a 'smart' doll named **Cayla had a security weakness** that could allow hackers to use it to steal personal data.

Do you know what you're looking for?

Training staff to spot an attack is key because relying on technology isn't enough. For example, at a basic level everyone should be aware of what spam emails and fake web pages look like. But we need to stop thinking of 'cybercrime' as a single entity, and crucially, it's not just something that happens to your computer.

It's about realising that cyber crime is actually part and parcel of a tangible, real-world web of scams and attacks that can cost you time, money and your reputation in the real world. Antivirus software and firewall programs can detect viruses, flag up some phishing attempts and spot system vulnerabilities, but you can't rely on them alone, or expect them to protect you against scammers actually tricking you in person.

Social engineering

Social engineering is a very common method of extracting credentials. Imagine a uniformed BT engineer turns up at your business premises, claiming your main phone line is down due to a problem in the area. You check the line – it's dead. Your customers can't get through and you're losing money, so how likely are you to let the engineer get on with the job? But what if they're an imposter? Hackers have been known to create crises for businesses, like cutting their phone lines, only to turn up and 'save the day' a few minutes later. What they're doing is getting potentially unlimited access to the business's network.

It's surprisingly easy – a hacker may ring up a company and speak to one member of staff to get hold of some seemingly harmless information. They then ring back on another line and speak to someone else, using that information to convince the person that they're legitimate. Having a few details to hand such as employee names and dates of birth means people are much more likely to trust them.

Ransomware

It's become common for smaller businesses to be targeted with ransomware too – a type of malicious software that blocks access to a computer system – a denial of service attack – or encrypts a user's files. It's used to demand money from people and only when they've paid up do they get their files back. Bigger organisations may be able to repel a ransomware attack (or swallow the cost) but that's not the case for smaller ones. If they find themselves with encrypted files and they're unable to run their business, the only real option may be to pay up.

Automated ransomware is becoming highly commoditised in a 'pile it high, sell it cheap' model that can be quickly replicated between machines. The **WannaCry attack in 2017** targeted Windows computers around the world, using hacking tools stolen from the US government to exploit a vulnerability and encrypt files in exchange for a bitcoin ransom. The attack affected 150 countries, with the hackers demanding $300 per infected computer to release files.

Phishing emails have become increasingly sophisticated too, the dodgy spelling and cut and paste layouts have improved dramatically and there's a newer trend to strike around big dates such as self-assessment tax deadlines. Then we have what's known as 'drive-bys' where an unwitting victim visits a website containing malicious code, which then downloads silently in the background.

The headline grabbers

It’s called zero day, because the weakness in the system hasn’t yet been uncovered by security firms, which means they’re like gold dust to hackers. Once a hacker discovers a zero day vulnerability, it’s a race for the anti-virus companies, software providers and cyber security firms to find a fix.

How protected are you?

All this may sound alarming but there are still practical steps you can take. If you outsource your cyber security, be sure your supplier is clear on how they’d handle an attack. How quickly can you apply a patch to your system? Do they have a procedure in place and are they on top of the latest developments in the industry?

While episodes like Shellshock are a worry, it’s important to be on top of existing, more everyday threats too, things like an SQL injection, one of the most common threats to businesses, caused by poor quality coding. The **Information Commissioner’s Office** can help with useful advice, but it’s also the institution charged with punishing firms for breaches, so it’s worth giving some time over to reading their guidance.

Let’s look at some of the other steps you can take today. They may not be able to prevent an attack, but they can help to make sure you’re better able to deal with it and get back to business.

Whether you’re a five-person operation or a five-hundred-person business, whoever’s in charge needs to step up when it comes to leading the charge on cyber security – it’s not a job that should be simply left to the IT crowd.

Cyber experts tend to have a formal cyber security strategy with clearly defined structures, processes and criteria. Your business should have a clear idea about the risks you face and how to manage them. For example, if you collect personal data, how is it stored? Is it protected? What would you do if it were compromised?

Does everyone in your organisation know they shouldn’t click on that suspicious-looking link or open an attachment from an unknown source? In a recent case, the Ministry of Justice was **fined £180,000** after suffering a data breach. The right encryption measures were in place – but nobody had turned them on. Don’t underestimate human error and don’t neglect strong identity authentication, aka **password management**.

Recording, tracking, documentation – these are areas where novice firms have scope to improve with only a moderate cost to the organisation. We found that while the overwhelming majority of experts (96%) say their organisation has a core source of cyber security guidelines in place, only 42% of novices are as well organised.

Your computers, tablets and smartphones can easily become infected by malware. You’re especially at risk if you’re using older, unsupported operating systems like Windows XP. Installing internet security like antivirus software helps protect them from hackers, viruses and other malicious software, but always download the latest software updates, it may be inconvenient but they contain vital security upgrades.

Be careful who you give details to, whether it’s on the phone, in person or online. If you receive an email with a link asking you to change your password for something like Facebook, don’t click – it could take you to a fake web page or allow ransomware to be downloaded to your computer. Instead, manually type the Facebook URL into your browser and see whether the website asks you to change your password.

1 Involve the boss

Whether you’re a five-person operation or a five-hundred-person business, whoever’s in charge needs to step up when it comes to leading the charge on cyber security – it’s not a job that should be simply left to the IT crowd.

2 Have a cyber strategy

Cyber experts tend to have a formal cyber security strategy with clearly defined structures, processes and criteria. Your business should have a clear idea about the risks you face and how to manage them. For example, if you collect personal data, how is it stored? Is it protected? What would you do if it were compromised?

3 Training

Does everyone in your organisation know they shouldn’t click on that suspicious-looking link or open an attachment from an unknown source?

4 Document your processes
Recording, tracking, documentation – these are areas where novice firms have scope to improve with only a moderate cost to the organisation. We found that while the overwhelming majority of experts (96%) say their organisation has a core source of cyber security guidelines in place, only 42% of novices are as well organised.

5 Tighten up technology
Your computers, tablets and smartphones can easily become infected by malware. You're especially at risk if you're using older, unsupported operating systems like Windows XP. Installing internet security like antivirus software helps protect them from hackers, viruses and other malicious software, but always download the latest software updates, it may be inconvenient but they contain vital security upgrades.

6 Always be vigilant
Be careful who you give details to, whether it's on the phone, in person or online. If you receive an email with a link asking you to change your password for something like Facebook, don't click – it could take you to a fake web page or allow ransomware to be downloaded to your computer. Instead, manually type the Facebook URL into your browser and see whether the website asks you to change your password.

Get a cyber insurance policy in place

Hacking activity is spread far and wide and it's being used for many different purposes across the globe, some of them very sinister. If a hacker broke into your business network and threatened to release your sensitive data, the costs and implications for you and your company could be catastrophic.

It's a serious business, but it's not all doom and gloom. If the worst should happen, having the right **cyber insurance policy** in place can help you investigate why and how the breach occurred and more importantly, how you can prevent it in future. Comprehensive cyber cover from Hiscox is available as part of our insurance for small businesses, it will put you directly in touch with experts, while we help you to get your business back to normal, assisting with legal costs, covering lost productivity and managing any reputational fallout.

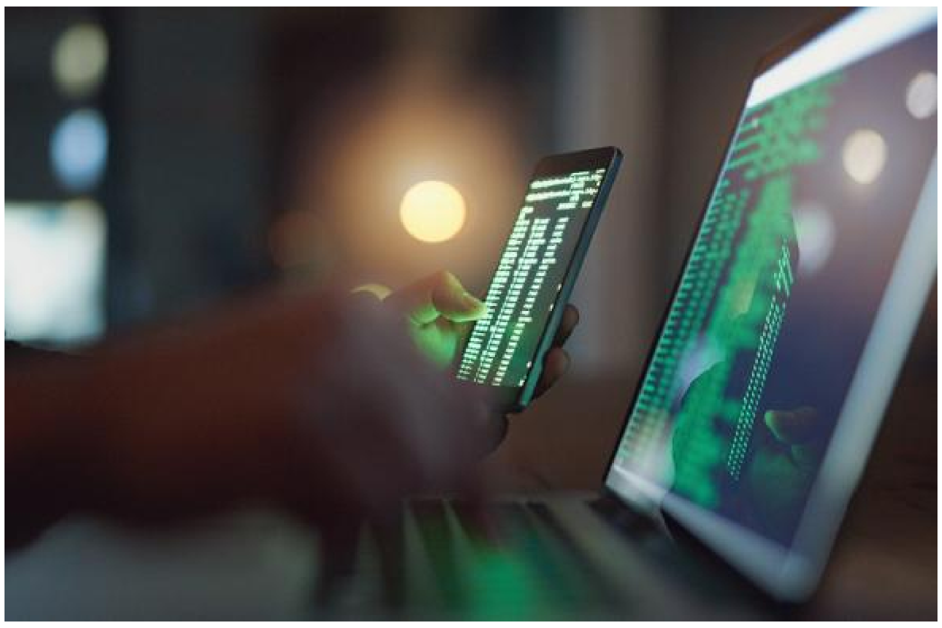
If you aren't confident your business is cyber ready, take the first steps to protect it with Hiscox Cyber Insurance or visit our **Hiscox Cyber Readiness Report Hub** to learn more.

Related articles

DATA AND TECH

Using analytics and big data to predict the future in your industry – The Bernard Marr column

Bernard Marr



DATA AND TECH

COVID-19 and cyber risk: Recent threats and scams

Hiscox Experts

DATA AND TECH

11 tips to prepare your business for the new EU data protection rules

Alex Wheal