Article

Jul 2022

Cybersecurity: de-risk your business

40% of businesses in Australia were the victims of cyber crime in 2021.



Kieran Fowler
Head of Cyber Consulting
Email kieran.fowler@waterstons.com

As we grow ever more dependent on the internet in our daily lives to communicate, research and store our data, and in the wake of shifting working practices due to Covid-19, the more opportunities cyber criminals have to exploit it.

The most common threat vector remains the humans themselves, as 83% of all attacks are phishing attempts.

With this increasing risk of cyber-attack, are you doing what you can to protect your business?

The figures

At the beginning of March 2022, it was reported that production at automotive giant Toyota shut all 14 of its Japanese factories after key parts supplier Kojima Industry was the target of a cyberattack.

For businesses, figures from the 2021 Verizon Data Breach Investigations Report found that a hacker can extract data from an entire customer database in a matter of hours, but on average it takes 200 days for an organisation to identify a breach – that's over six months. Six months that the hacker still has access to your system, and data.

Here are the key takeaways from the 2022 DCMS Cybersecurity Breaches Survey:

- More than a third (39%) of all UK businesses are being attacked in any given year.
- 83% of all organisations surveyed said they'd experienced some form of phishing attack in the last 12 months.
- Up to 80% of cyberattacks now begin in the supply chain. Only 13% of businesses assessed the risks posed by their immediate suppliers.
- The average cost of a breach across businesses of all sizes is £4,200, with a figure of £3,080 for SMEs. If you're a medium or large-sized business, the average figure stands at an eye-watering £19,400.
- While 57% of large firms have a formal information security strategy, just 20% of micro firms and 37% of small firms have one.
- Just 19% of businesses surveyed said they had a formal incident response plan. One in five businesses (19%) stated they were not sure what they would do during a ransomware attack.
- Only 6% of businesses have the Cyber Essentials certification and just 1% have Cyber Essentials Plus.

Cyber criminals are usually looking for something specific; personal data of customers, a firm's intellectual property, employee data or financial information. This data is valuable to you as a business, but even more so as leverage for a hacker.

So, what can you do about it?

Audit

When was the last time you looked at your corporate systems and the data that is stored within them? Who has access to it? Is that access protected?

As the UK, and world, is finding the new normal following the response to working practices in Covid lockdowns, now is the time to make sure you ask yourself simple questions in relation to your data:

- What is stored?
- Where is it stored?
- Why do we have that data? Why is it stored there?
- Who can access this data?
- How is the data protected?

These questions can help you identify the weaknesses in your system, where improvements can be made, and the most significant areas of concern.

Plan

Where to start?

Make sure you're following a framework! Our MD Charlie has put together a list to help you protect your business and prepare for the future. Take a look at what suits your firm best here.

Using guides like these and understanding the security risks that your organisation might have is crucial to your cyber security planning, but it's important to remember they are by no means exhaustive, and may not always be relevant to your business, which is why it's important to ensure that you are creating a dedicated, bespoke plan that works for you.

Fitting with your organisation and structure, your plan should consider points such as:

- Communication channels
- Who has access to data and how
- What are most valuable systems and data
- How to protect your data
- What to do in the event of a breach
- Where do you sit in the supply chain

Prioritise

All businesses have different strategic objectives; figure out what yours are and what critical functions you need to prioritise and protect.

A prime example is the manufacturing sector. It is a target for cyber criminals due to the significance of its supply chain and how one part of it cannot be out of action for an extended period of time before havoc is wreaked.

This short lead time, and costly down time, is appealing to hackers as it usually results in speedily paid ransoms in order to get the industry, sector, and sometimes even country, back on track.

For example, if a manufacturer of pharmaceuticals was hacked and unable to produce medication, it cannot be shipped, distributed or prescribed, potentially crippling the healthcare system.

The strategic business objective in this example is delivering drugs to clients in need. The critical business function is manufacturing and therefore, the priority should be securing that supply chain.

Alternatively, your priority may be on securing sensitive data. Do you have multi-factor authentication in place for all team members across all systems? Small changes such as the ease of accessibility could have a huge impact in your vulnerability to cyber-attacks.

If you are renowned for your research and development, innovative ideas and revolutionary impact; is protecting your wider reputation and reliability your key priority?

Visualise

Cyberattacks, security solutions, threat levels and the general sophistication of systems are always changing. With every new technology comes a new way for our data and systems to be compromised, so ensuring that you are prepared is vital.

This visualisation does not simply extend to your reaction to threats, but also the prevention of them.

For example, what are you working on? What are the future plans for your business? Do these leave you open to a security breach? Will competitors, hackers or general criminals want to know how and when your plans will be implemented? Who do you work with that can have an impact from further away?

The global 'WannaCry' ransomware attack found its way onto computers systems within the UK's National Health Service (NHS), disrupting more than 80 hospitals and 8% of GP practices. This caused mass disruption with 19,000 appointments being cancelled and costing the NHS £92m to correct.

This malware spread and a newer variant of that same ransomware later forced the Taiwan Semiconductor Manufacturing Company to temporarily shut down several chip fabrication facilities. The knock-on effect did not help the global computer chip shortage and Apple had to cut the production of their latest iPhones.

So, it's important to think of what can occur globally that can have an impact on your business locally and be as prepared as possible.

Regardless of whether you consider it compromising to your operation, having an overarching view and understanding of what others deem valuable, and finding ways to protect them is key.

After all, would you leave your car keys sitting by an open window, or your best jewels on display in your car? Probably not, so why leave the door open for cyber criminals?

There is no denying the cybercrime is rife and is only becoming more prevalent; after all 39% UK businesses had experienced a cyber-attack in the past year.

While there are measures you can implement directly and in house, working with an external expert ensures you have access to the latest knowledge and protection. No matter what your budget, there is a solution for you.

To find out more about cyber security and how our team can protect your business now and in the future, visit our Cyber Security page here.