[Basic guide to Cybersecurity]

Everything you need to know about business cybersecurity

BACK TO BASICS

[Introduction]

Why is cybersecurity so important?

Just as the pandemic made us all more dependent on the internet, so it made us more vulnerable to cyberattack.

In the first 12 months of the pandemic, 39% of UK businesses and 26% of charities reported cybersecurity attacks or breaches.

According to the Government's annual Cybersecurity Breaches survey, "the risk level is potentially higher than ever (because) businesses are finding it harder to administer cyber security measures."

This increased level of threat won't fade with the pandemic. Organisations of all sizes continue to invest more in digital tools that facilitate remote work, e-commerce and digital transformation.

By doing so, they're creating more efficient and resilient operations. But they're also opening back doors to their data that might not have existed two or three years ago.

In 2022 and beyond, comprehensive cybersecurity is a must-have, regardless of your size or sector. One study found that a million small UK businesses would be at risk of collapse if they were forced to deal with the average costs of a cyberattack.

In the rest of this paper, we'll examine the risks SMEs face, and what they can do to avoid falling victim to a new generation of cyber threats.

39%

of UK organisations fell victim to some form of cyberattack in 2022

[The changing cybersecurity environment]

In some respects, the threats SMEs face today are similar to the threats they faced in 2019. But hackers have been emboldened by the widespread switch to remote working and our increasing reliance on digital tools. They have become adept at targeting the new vulnerabilities these trends create.

Remote workers

Remote work is here to stay - mostly in hybrid form - because employees want it and businesses can see benefits in terms of recruitment, retention and cost. But the Government's Cybersecurity Breaches survey suggests that the switch to home and hybrid working is making it harder for on-site IT teams to monitor users for behaviour that might make networks vulnerable to attack.

It's easy to see why that might be. Working from home, away from the watchful gaze of IT staff, makes it more likely that users will download unsanctioned software or thoughtlessly click on an unsolicited email link. It's harder to enforce security protocols with a dispersed workforce.

To make matters worse, remote work means there are fewer opportunities for IT staff to patch and update connected devices and check they are running the latest and most secure versions of apps and services.

The rise of BYOD

At the same time, more businesses have sanctioned the use of personal devices for work use. This has led to cost efficiencies - and security challenges. Many companies don't have comprehensive Bring Your Own Device (BYOD) policies that ensure personal smartphones, tablets and laptops are used in a secure way. The result is that more employees are connecting to company networks from devices that offer consumer grade security at best.

81%

of UK organisations don't have a formal incident response plan

The growing threat of ransomware

According to PWC research, 61% of executives expect to see an increase in ransomware incidents in 2022.

Ransomware typically involves the inadvertent downloading of malicious software that locks businesses out of their data and services until a ransom is paid. It is usually the result of a phishing attack, in which employees are tricked into downloading the malware onto their computers, from where it spreads across the IT estate.

We know that criminals have ramped up phishing attacks in the last two years. One report also makes it clear that phishing attacks are becoming more sophisticated. It states: "As attackers work to make their phishing attacks more targeted and effective, they've started researching potential victims, working to collect information that will help them improve the odds that their attacks will succeed."

Again, this growing threat is partly the result of a changing digital landscape. Phishing attacks often target remote workers without easy access to IT support.

Third Party Vulnerabilities

Remote work is here to stay - mostly in hybrid form - because employees want it and businesses can see benefits in terms of recruitment, retention and cost. But the Government's Cybersecurity Breaches survey suggests that the switch to home and hybrid working is making it harder for on-site IT teams to monitor users for behaviour that might make networks vulnerable to attack.

It's easy to see why that might be. Working from home, away from the watchful gaze of IT staff, makes it more likely that users will download unsanctioned software or thoughtlessly click on an unsolicited email link. It's harder to enforce security protocols with a dispersed workforce.

To make matters worse, remote work means there are fewer opportunities for IT staff to patch and update connected devices and check they are running the latest and most secure versions of apps and services.

82%

of UK business leaders rate cybersecurity as a 'very high' or 'fairly high' priority

[The basics of protection]

In this environment, it's encouraging that, in general, most organisations take cybersecurity seriously. According to the UK Government research, 77% of businesses say cybersecurity is a high priority for their directors or senior managers.

But in a fast changing world, many smaller organisations in particular don't feel they have the time, expertise or energy to research and implement an all-encompassing security strategy. Instead, they install basic antivirus software and a firewall and hope for the best.

That's no longer enough, but the good news is that protecting your business may not be as complex or costly as you think. In fact, a few well executed fundamentals can go a long way.

Education

According to a Verizon report, 85% of data breaches involve human error. Phishing attacks are increasing because cyber criminals know they work. The very best way to guard against phishing attacks is through employee education.

That needn't be complex or costly. Create security rules specifically for a remote or hybrid workforce, then write them down and make sure every employee reads them. Include a BYOD policy, and update the rules whenever necessary. Send priority alerts about the latest cyber threats, and include cybersecurity reminders in the staff newsletter or at staff meetings.

Your rules should include the usual advice about spotting malicious emails and treating unsolicited contact with caution. It might also include lists of sanctioned and unsanctioned software and services.

Culture

A corporate culture that encourages open and honest debate around cybersecurity is one of the best ways to counter its threat.

Emphasise that employees are the first line of defence against cyberthreats, and give them the resources to properly fulfil that role. If possible, expand IT helpdesk support (either in-house or outsourced) and encourage staff to say when they need extra help.

Employees shouldn't feel embarrassed putting up their hands and admitting to confusion around even basic cybersecurity issues.

Technology

Along with educating employees and creating a safety-first culture, you need to invest in the tools to keep your data and services safe. That includes, as a minimum, good antivirus software, an enterprise-grade firewall and a fit-for-purpose Virtual Private Network (VPN).

A VPN offers the ability to encrypt and secure traffic between any device and a VPN server, meaning your data can't be stolen in transit when remote employees connect to your central network.

[Managed Security Services]

Why consider them?

In this environment, it's encouraging that, in general, most organisations take cybersecurity seriously. According to the UK Government research, 77% of businesses say cybersecurity is a high priority for their directors or senior managers.

But in a fast changing world, many smaller organisations in particular don't feel they have the time, expertise or energy to research and implement an all-encompassing security strategy. Instead, they install basic antivirus software and a firewall and hope for the best.

That's no longer enough, but the good news is that protecting your business may not be as complex or costly as you think. In fact, a few well executed fundamentals can go a long way.

£4,200

is the average estimated cost of all cyber attacks during 2021

Managed security from Vaioni

Vaioni's own Managed Firewall solution offers 24/7 intrusion monitoring, real time anti-spam and malware, and a powerful VPN that extends protection to remote or mobile employees. It protects both computers and mobile devices, and everything is managed from a simple web portal, accessible anytime and anywhere.

Vaioni also offers Unified Threat Management, which offers end-to-end security across your infrastructure, automated intrusion prevention, advanced threat detection and protection that extends to all your employees' devices, whether company-owned or BYOD.

These are powerful solutions that don't just tackle age-old issues around cybersecurity: they update your security to include new challenges around remote work, BYOD and the huge increase in reliance on cloud-based tools. In other words, they upgrade your security for the challenges of today, and for the challenges that will exist for years to come.

[The takeaway]

The cybersecurity landscape has changed, and if anything it's more dangerous terrain than ever before. Criminals are all too aware of the changes to working patterns and technology use brought about - or at least hugely accelerated - by the pandemic, and have honed their attacks in response.

It's up to every business to prime their defences to counter this threat. A head in the sand approach is a disaster waiting to happen. Cybercriminals who can buy off-the-shelf malware for a few pounds on the dark web don't care if you're a small, local operation with modest revenues. To some hackers, that just makes you an easy target.

No organisation can take security for granted. You need to educate your staff, and if necessary invest in appropriate training. Create a culture that recognises and rewards good cybersecurity practice, and always has an eye on emerging threats. Finally, invest in tools that maximise your protection and minimise the chances of a data breach. Even a partial breach is likely to cost far more than the price of decent security software.

If you need help with any of that, Vaioni is happy to guide you through the options available, with no obligation. We offer a full suite of managed security services that give enterprise-grade protection at a sensible price. Our specialists take over the task of monitoring your network and managing your security infrastructure.

Vaioni also offers communications and connectivity services, so we can design a complete end-to-end digital infrastructure that precisely meets your needs.

If you'd like to know more, please get in touch.

0161 672 9900

www.Vaioni.com

sales@vaioni.com

39%

of UK organisations fell victim to some form of cyberattack in 2022