Five cyber security best practices every small business should know

As more and more of our lives migrate online, the reality is that cybersecurity now a vital consideration for every type of business, regardless of size or sector.

This is especially pertinent for the inherently vulnerable small business community without the technological defences or security intel needed to ward of attacks. But, the good news, according to Chris Pottrell founder and MD of *Nebula* IT consultancy, is that there are some relatively simple and cost-effective measures small business owners can to take to better themselves:

It's no secret that the past two years have seen our society become even more, if not entirely dependent, on the continued availability of connected technologies amid the rapid shift of work to remote and hybrid offices. But as well as significant benefits, the increasing rate of digitalisation has enabled cybercrimes to be committed in newer, more creative ways as hackers take advantage of the vulnerabilities and gaps in security by businesses.

The result is that cybercrime continues to grow at pace. Last year a national study estimated that 39 per cent of all UK businesses had encountered a cyber-attack over the past 12 months coming in at an *average cost of £4,200*. Worse still, Google's 2023 cybersecurity predictions expect this illicit economy will only continue to expand and diversify.

And this issue is even bigger for small businesses. This is because they often have fewer resources and lack security expertise, leaving them even more

exposed to the latest online scams and attacks. In fact, of all cyberattacks it's estimated 43% target small businesses and SME startups – with *60% going out of business within six months*.

As such, it's more important than ever for small businesses not to overlook investing in cybersecurity, both technology and user education. Fortunately, there are some basic cyber defences that can help to protect any small enterprise:

1. Make cybersecurity awareness a priority. Phishing and viruses are two common methods of attack and, perhaps surprisingly, these types of breaches are typically caused by human error. Whether through haste or lack of awareness, it's your own employees who pose the biggest threat to your IT infrastructure. That's why it's so important to take a proactive, ongoing approach to educating your entire workforce about cyber security threats and countermeasures. This should include regular cybersecurity training sessions. Your employees should understand how published information about your systems and operation can reveal potential vulnerabilities. This should be supported with easy-to-follow procedures for employees designed to help mitigate the risk. Ensure they are alert to suspicious emails, even those purporting to be from trustworthy sources, delete them without clicking and notify IT; allow only a few to have access to confidential information; choose strong passwords and keep them stored safely and separately; install secure configuration to minimise the information that digital devices disclose and back up data regularly, so it can be retrieved should a crisis occur.
2. Ensure all the cybersecurity basics are in place. Beyond developing an employee-centric security approach, there are a range of network security measures every business should take. This should start with secure network design; applying network perimeter defences to block out any insecure or unnecessary websites and services, along with malware protection to block malicious emails and prevent malware being downloaded from websites. It also means enforcing VPN for remote access, encryption-in-transit and for data-at-rest, and authenticating all users access. You could also institute least-privilege security so that each employee is only granted the minimum system resources and authorisations they need to perform the job in hand. This means if a user account becomes compromised (such as through phishing) or a computer system is hacked (such as by exploiting a zero-day vulnerability), you can help contain the damage.
3. Ensure breaches can be managed effectively. Now that you have the basics in place, you should be well placed to successfully exploit and mitigate known vulnerabilities with just a few controls. This means applying patches and fixes to operating systems, applications and drivers to prevent attacks which exploit software bugs. It should also entail

introducing additional malware protection on the internal network at key points of vulnerability. This sounds simplistic, but failure to conduct these types of updates in a timely fashion is a leading cause of breaches.

4. Monitor and analyse the network. Business owners cannot afford to underestimate the importance of continuing to monitor their network in order to detect and address anomalies. This should involve keeping a log of everything – every transaction, every privileged login to your network, every failed password attempt. Collecting this information and making it available for analysis will not only help detect and address a breach before it escalates into something bigger, but to pre-empt similar points of entry or system constraints – and take the appropriate remedial action.
5. Keep a finger on the pulse at all times. One of the most important concepts to grasp with cybersecurity is that maintenance is a constant job. New attacks develop monthly, if not daily, and your approach to guarding against them must be constant. That's why, even though the aforementioned measures will safeguard you from the majority of standard attacks, it's crucial not to get complacent and keep a finger on the pulse. This means maintaining a good understanding of what constitutes 'normal' activity on your network (see point 4) and ensure a rapid response to even the slightest anomalies. As part of this, conduct pen tests regularly and thoroughly; not only do systems become less secure if not maintained properly but attackers become more sophisticated.

Whilst these actions do not guarantee you will not be hit, they will greatly minimise the growing cyber risk for your small business – helping your small business continue to grow without becoming another cybercrime statistic.

Cyber security is a complex issue and if you're unsure on managing the risks then get in touch at enquiries@nebulaIT.com. For further information please visit *https://nebulait.co.uk*

Chris Pottrell is the founder and MD of *Nebula* IT consultancy.

Article by CHRIS POTTREL