The state of small business cybersecurity

As businesses look towards their post-pandemic future, has COVID impacted their cybersecurity? Have new threats been revealed? And what does post-COVID cybersecurity look like?

Temps de lecture : minute

6 October 2021

According to the current *Cyber Security Breaches Survey* from Sonicwall, four in ten businesses (39%) report having cybersecurity breaches or attacks in the last 12 months. The most common are phishing attacks (83%), followed by impersonation (27%). And there is a tangible cost to these breaches, with the average cost of a security incident being £8,460.

The pandemic switched the attention of all business leaders to re-organise their workforces and their networks with often less than comprehensive security measures in place. In addition, the challenges of massively changing business processes to mitigate the impact of the pandemic made many enterprises vulnerable to attack.

NCSC (National Cyber Security Centre) spokesperson told Maddyness that small businesses must always be vigilant and take practical action to secure their systems: “Cybersecurity should be considered a priority for all organisations as the consequences of an attack can be very severe, impacting finances, operations and reputation. Our *free Cyber Action Plan tool* is designed to help small businesses identify areas for improvement. And we encourage SMEs to familiarise themselves with our *Small Business Guide* which sets out practical advice on how to secure their operations online.”

The digital footprints of small enterprises have been diversifying for the past decade. As the threat landscape has evolved, so too have the sophistication of attacks on all business sizes.

“The increased frequency of cyberattacks on smaller enterprises has come as a direct result of the pandemic,” Craig Lurey, CTO and Co-founder, Keeper Security, tells Maddyness. “The sudden introduction of restrictions meant that businesses both large and small were forced to shift to remote work at short notice, thereby pushing CIOs and CISOs to hurriedly update their company’s cybersecurity policy. However, due to a lack of resources, SMBs were more negatively impacted by this accelerated change and were left with gaps in their defences, which opened them up to cyberattacks.”

It’s clear that the threat landscape has changed and diversified. Small businesses, though, are not powerless to act. Understanding what constitutes robust and comprehensive cybersecurity is the first step to an integrated policy. Considering the tech stack in use across a small business’s network footprint will reveal weak areas that need attention.

Evolving threats

As the threat perimeter businesses had to secure shifted to the homes of their workforces, this posed additional cybersecurity challenges that remain a clear and present danger to their networks. As businesses re-draw their digital transformation roadmaps in the wake of the pandemic, cybersecurity must be front of mind.

Also, as the results of a *BBC* survey suggest, nearly three-quarters of workers believe they will never return to their offices full time, a comprehensive, integrated and robust security systems must be in place

to protect these legions of workers.

Speaking to Maddyness, Adam Strange, data classification specialist at HelpSystems, explains why network access security is of paramount importance: "Forrester reports that lost, stolen, or compromised privileged credentials are involved in over 80% of all enterprise data breaches, making this an increasingly major issue across the entire business landscape. Often flying under the security radar, these privileges create security blind spots that can potentially lead to devastating breaches."

More investment in cybersecurity must be a priority. However, the Keeper Security survey is worrying as it revealed that almost all (92%) UK organisations are aware of where the gaps or weak links in their cybersecurity defences are, but fewer than half (40%) are actively addressing all of them. However, encouragingly *ConnectWise* found that small businesses would pay on average 34% more for an IT service provider who could provide the right solution, a rise from 25% in 2019.

Look closely at your business's current security profile and the services in use to secure these systems. Are they fit for purpose? Could your business combat one of the many types of cyberattacks that could be targeted at your enterprise? A complete security audit will reveal these weaknesses. With this data, a new cybersecurity stack can be defined and deployed.

Protect and secure

UK businesses are under attack. The SonicWall Cyber Threat report concludes the UK was the second most-hit country globally for ransomware, suffering 14,603,315 hits in the last six months, with

ransomware spiking by 144%.

Often, smaller enterprises will have embraced the cloud as it offers a multitude of hosted low-cost and scalable services. However, the wholesale adoption of the cloud as a central component of many small business's networks and data strategies has left many vulnerable to various threat actors.

NCSC explained to Maddyness that taking a more holistic approach to cybersecurity is needed: “Modern small businesses do not typically have complex, in-house IT set-ups, unless they have specific needs, and instead generally take a ‘cloud-first’ approach. In practice, that means they often rely on the security measures built-in to their local Wi-Fi or phone networks, devices, and cloud services to protect themselves online. These security features provide a good baseline level of protection against common cyber threats; however, it’s important for small businesses to ensure these protections are configured properly and turned on, such as firewalls and filtering options.”

To combat the cybersecurity threats small businesses face, business leaders often indicate a lack of security skills as challenging. Indeed, according to *Keeper Security*, “A key challenge for UK companies is a lack of cybersecurity skills. Nearly a quarter (23%) of all organisations believe that they don’t have the right skills within the business to adequately protect themselves against cyberattacks.”

John Smith, director, Solution Architect, Veracode commented on the government’s recent announcement to invest £700,000 to boost cyber skills: “It’s great to see the government is investing £700k to help develop cyber skills in the UK. The current technology skills shortage, especially in security, has been a pressing issue for some time. It’s clear that more needs to be done to prepare for and mitigate the impact of cyberattacks - there are currently only five undergraduate computer

science degrees certified by the UK’s NCSC for cybersecurity content.”

The importance of cybersecurity resilience, particularly across the small enterprise sector, can't be overstated. A clear post-COVID challenge is creating flexible networks that support remote working, continue to leverage the cloud, yet deliver robust security policies reinforced by good cybersecurity behaviour. The cybersecurity threats businesses face has evolved. Those companies that invest today to secure their workers and systems will thrive in the post-pandemic digital landscape.

Article by David Howell