

Why Cybersecurity Needs to be Prioritised as Small Businesses Face the Cost-of-Living Crisis

You're reading Entrepreneur Europe, an international franchise of Entrepreneur Media.

Written by Marcin Kleczynski, CEO & founder, Malwarebytes

As the spectre of a recession looms, the sting is being felt by startups, scaleups, and other small businesses. In the UK, prior to her resignation, former Prime Minister Liz Truss announced that energy bills would be cut by half over winter. This undoubtedly helped mitigate some concerns; against the backdrop of rising inflation, smaller organisations need all the help they can get.

As wallets become thinner, it might seem tempting to cut costs on security. However, this can spell disaster, especially for small businesses; more than half (60%) go bust within six months of getting hacked.

This is a particularly pressing issue in Europe, which has seen a gradual uptick in cybersecurity attacks in the last decade. Companies must protect themselves against cybersecurity risks and not push them to the bottom of the pile. Most notably, ransomware attacks are on the rise, persisting as the primary method of cyber intrusion, thanks to the sheer financial gain that fraudsters stand to make from exploiting users. In Britain alone, the estimated cost of attacks is £27bn per year. It's no wonder, then, that demand

for cybersecurity roles in the UK increased by 22% in the last year – but skills gaps can make these roles hard to fill.

The tight budgets that early-stage founders are operating with exacerbate this. As cybercriminals get richer, businesses' finances are dwindling as they fight another battle: the cost-of-living crisis. With increased electricity costs weakening bricks and mortar-based businesses, and the ongoing question of how much to balance salaries against rising inflation without gutting the business, it's a difficult time for all entrepreneurs. Small businesses must learn a stern lesson: failing to prepare is preparing to fail.

Why small businesses are targets.

Beyond underestimating the threats small businesses face, with only 26% believing it is a top priority, there are several reasons why smaller organisations are particularly vulnerable. The key distinction between small businesses and larger corporations is the lack of access to resources. Scant assets or knowledge of how cybersecurity works, as well as not knowing which software best suits, puts smaller businesses on the back foot. Thanks to multiple vulnerabilities left unchecked, small businesses often receive more attacks than larger, better-equipped counterparts. Robust security infrastructure is needed, yet over 40 percent have no in-house IT personnel.

Ransomware is one of the primary threats small businesses face, worsened by the cost-of-living crisis. Already in a fragile financial state, there is rarely enough budget to pay ransomware fees. Times of uncertainty create perfect conditions for cybercriminals to capitalise on. Vulnerable organisations are cornered by criminals and forced to either pay large sums of money or risk the exposure of important data.

Another weapon deployed by cybercriminals is phishing, whereby

criminals trick recipients into thinking they're talking to someone they know through scam emails, texts, or phone calls. Attacks have become far more advanced than attaching a dubious link to an email, causing an employee to download malware. Now, vast amounts of sensitive data can be exposed. Small businesses and their employees may not possess the expertise to identify these links; that is why they receive roughly 4,500 suspicious emails every day.

How to strengthen defences.

To stand the best chance of fighting cyber criminals, first and foremost, regularly backup all critical data. Should a ransomware attack occur, backups will minimise the damage, saving time and money. In turn, encrypting communications will help prevent third-parties from intercepting important data.

Next, for those using Microsoft, pay attention to Patch Tuesday, Microsoft's monthly release of security fixes for the Windows operating system (OS) and other software. Out-of-date software quickly becomes riddled with vulnerabilities, which is why Microsoft users are advised to download and patch their systems from the official website.

Moreover, with smaller firms more likely to have hybrid or even remote-first working environments, endpoint protection is crucial. Installing the right software with prevention capabilities developed specifically for resource-constrained companies can reduce attack surfaces. A cloud-hosted approach enables centralised management of endpoint protection, which detects and responds to threats swiftly. The best solutions also remove all traces of the offending attack (such as malware) and expunge any residual files, code or configuration changes that might otherwise be missed.

Combining artificial intelligence (AI) with human heroes is the best way to detect and remediate threats. After all, everyone being aware of all security threats is not realistic,

so it's essential to get ahead with AI-powered technology that fights cybercriminals in the background. For a helping hand, smaller firms grappling with the growing complexity of maintaining GDPR compliance across multiplying digital threat surfaces – exacerbated by a lack of internal security talent – should find solace in managed service providers (MSPs).

MSPs equip small businesses with a cost-effective and fully-fledged security team to protect against infections and reduce exposure. MSPs can be critical collaborators in helping start-ups, scaleups, and other early-stage companies overcome security challenges. As well as protecting against attacks, the right MSP will help founders achieve critical business goals, which will help keep the business thriving for many years to come.

Beyond technology.

There is no doubt that technology provides the most efficient way of dealing with cyber threats. However, with the cost-of-living crisis hitting parts of Europe harder than anywhere else in the world, employees might be increasingly distracted – which is where hackers can pounce. Cyber criminals don't hold back when faced with economic trouble; in fact, they usually double down on efforts. Just this month, the National Cyber Security Centre (NCSC) – part of intelligence agency GCHQ – revealed that scammers are exploiting this crisis, tailoring phishing attempts by impersonating the government, HMRC, and energy regulator Ofgem.

Constant vigilance is vital. Effective cybersecurity employee education programmes that combat fear fatigue elevate cybersecurity as a strategic priority, ensuring vigilance; 88% of cyberattacks stem from employee errors, so work with them to help sharpen threat awareness.

Gamifying security training, including phishing employees, can make a big difference. Staff are easy targets, so phishing

simulation testing can be a productive way to teach them what a malicious link looks like. People generally respond well to many aspects of gamification, so it could speed up understanding of the evolving threat landscape, increasing awareness.

Managing the cost-of-living crisis is difficult enough for small businesses. Layering up security networks and enhancing employees' cybersecurity awareness could save organisations. European firms are understandably cutting budgets in different departments to navigate these tough times, but founders won't do themselves any favours by lowering security costs.

<https://www.entrepreneur.com/en-gb/science-technology/why-cybersecurity-needs-to-be-prioritised-as-small/446651>