VCG

cisco Partner

A small business guide to cyber security

Protecting your people, data and devices

According to the UK Government's National Cyber Security Centre, as an SME there is about a 1 in 2 chance that you'll experience a cyber security breach. The EU Agency for Cybersecurity has also identified that while the majority of SMEs use some security controls – backups, antivirus protection and firewalls – far fewer train all their employees about the risks, or utilise logging and alerting systems.
Most SMEs do not perceive cyber-attacks as a major risk – and many consider that only larger companies are targeted.

That's not the case.

- UK small businesses targeted with **65,000** attempted cyber attacks per day.

  Source: Hiscox

- Cyber breaches cost the average small business **£25,700** in basic 'clear up' costs every year

  Source: CSO Online

- **44%** Customers in the UK will stop doing business with a company that was involved in a cyber attack

  Source: CSO Online

The odds of SMEs being targeted have been exacerbated by the need to work from home in 2020/21 and the desire for organisations to enable an increasingly remote workforce.
The speed of change has been rapid, and this has undoubtedly left many organisations reverse engineering their security. Working from anywhere on multiple devices provides the flexibility that most want to do their job, but security is too often an after-thought.
The vast array of devices – both personal and corporate, presents a huge security risk.

Smart companies prioritise cyber security to prevent data loss, avoid PR embarrassment and the remediation costs that come with associated breaches. Having a company policy for best cyber security implementation should be best practice so that employees know what constitutes good and bad use of systems and software, potentially leaving the organisation open to risk.

So where should you put the most focus when keeping your business safe, secure and operational?

Here are a few tips on how you can achieve that:

Data Loss Prevention

Preventing the loss of your company data doesn't just come from external cyber security threats, it can also be from insider threats – targeted or not. Everything from a disgruntled employee, to user error, to those employees that skipped cyber security awareness training and are ignorant to the threats – they all represent risk to your data.

Taking regular backups of your data so that it may be restored in the event of a breach will reduce both the inconvenience of data loss from theft, fire, ransomware or any other damage. Identifying what is most important – documents, files, databases, calendars and contacts means those assets that are key to keeping the business operational are routinely secured.

Identify secure data storage options separate from company offices, so if there is physical damage to systems (fire, flood, theft), the data is secure in a separate location and can be restored. Cloud back up is also simpler to access from anywhere and can make the difference between days and just a matter of hours to be operational again.

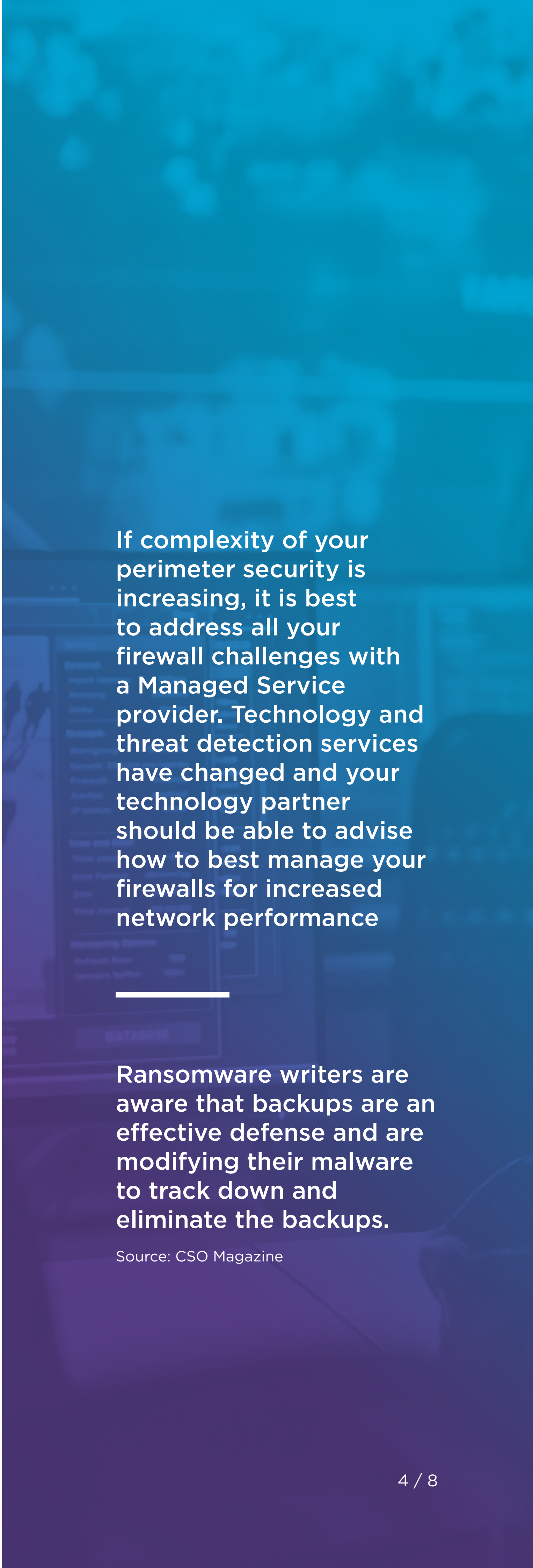
Malware

You can protect your organisation from the damage caused by malware and viruses by adopting a number of simple and cost-effective good practices.

Firstly, use antivirus software on all computers and laptops. Devices must be kept up to date – making sure the latest versions of software are installed when prompted, as they often contain security patches and upgrades. When installing software on devices such as smartphones and tablets make sure it's approved software. Stipulate in company policy that third party apps from unknown sources pose a risk to data and should not be downloaded.

Make sure all software and firmware are patched when prompted to do so by the vendor. Automatic updates can be actioned so that where possible, human error can be eradicated. Similarly, ensure the firewall between your network and the internet is on.

Finally, most data loss horror stories involve the downloading of data onto USB sticks or other removable media. It's worthwhile disabling ports on devices so that downloading of data is unavailable to most. Data that needs transferring should be shared across email or via cloud storage systems which are heavily backed up to eradicate the risk of losing the media – and thus the data too.



If complexity of your perimeter security is increasing, it is best to address all your firewall challenges with a Managed Service provider. Technology and threat detection services have changed and your technology partner should be able to advise how to best manage your firewalls for increased network performance

Ransomware writers are aware that backups are an effective defense and are modifying their malware to track down and eliminate the backups.

Source: CSO Magazine

Email and phishing attacks

According to the National Cyber Security Centre, the UK saw a 15-fold rise in the removal of online scam campaigns in 2020 compared with 2019. It has taken down more scams in the last year than in the previous three years combined.

48% of malicious email attachments are office files.

Smaller organisations (1–250 employees) have the highest targeted malicious email rate at 1 in 323.

Source: Symantec

Emails containing bad links and requesting personal data have become an enormous headache in their own right for SMEs, and increasingly one of the best ways to target them as an organisation is to train employees how to spot them and be vigilant.

They're often easy to see as they contain poor spelling, bad grammar and low-quality versions of recognisable logos. The email addresses don't look legitimate - or they purport to be from a known contact.

Ensuring employees don't browse the web or check emails from accounts that have administrator privileges will reduce the impact of successful phishing attacks. Where attacks may have been successful, it's important to change passwords and to be supportive to employees – it's important they report problems without fear of retribution.

Passwords and two factor authentication

For very little effort, password management is the simplest way to prevent unauthorised people from accessing devices or data. It adds a large amount of security for little cost or time. Making sure they're regularly updated and aren't predictable (there are many random password generator websites) and reporting password breaches to IT as soon as possible.

Encryption products, fingerprint or facial recognition also help reduce data loss. Two factor authentication (2FA) requires two different methods to prove identity before using a service. We're increasingly seeing the use of pin codes sent to our smartphones to verify our identity. Banking has put 2FA to use with card readers that require information in addition to a password.

If security feels overwhelming both in knowledge and time to you and your employees, then there is another option. You can work with a partner who has cyber security expert knowledge, the resources and time to put those skills to good use.

Cyber security consultancy services for SME

Evolve and unify your security operations

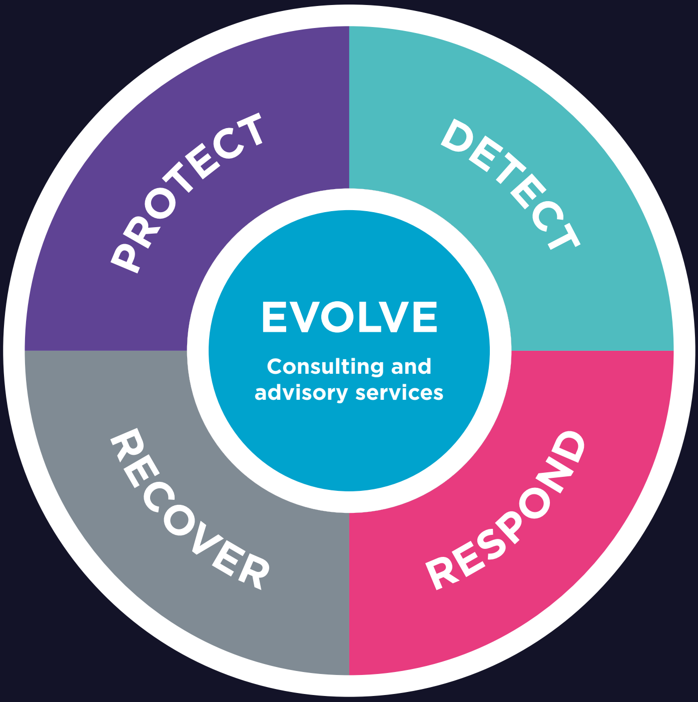
VCG helps organisations discover the wide range of possibilities to help them stay compliant and become cyber resilient with consultancy and advisory services and solutions that can help protect the entire network, devices, locations and operations.

Our service model brings cybersecurity at the core of our portfolio. We help businesses unify their plans and strategy across people, devices and locations in a single approach: consult, design and evolve cyber security for the organisations we work with.

VCG
Security lifecycle:

Our portfolio of solutions and services help SMEs:

- Evolve cyber security strategy
- Mitigate cybercrime and continuously adapt to evolving malware and cyber threats
- Unify protection across networks and cloud environments



Protect

Our services include perimeter security, Security Service Access Edge (SASE), network and identity access, end point protection and secure web access to keep your organisation protected around the clock.

Detect

Threat intelligence helps to mitigate risks before they happen so you can rest assured your network is protected. Our managed threat detection and response services (SIEM) help monitor and alert for any threats, providing 24 x 7 availability and expertise to pre-empt and respond to cyber threats

Respond

We respond to the threats via a 24/7 SOC as a service for incident management and breaches. We respond so you know experts are in control when there is an imminent threat.

Recover

Business continuity and disaster recovery services, including back up and disaster recovery as-a-service.

Benefit from integrated security solutions to cover all layers of defence, on premise and in the Cloud; Unified threat management capabilities and the right technology and vendors to suit your needs

Shaping your **next**
in technology and IT

Contact us today

Email	sales@vcg.group
Tel	0161 406 1820
Website	vcg.group