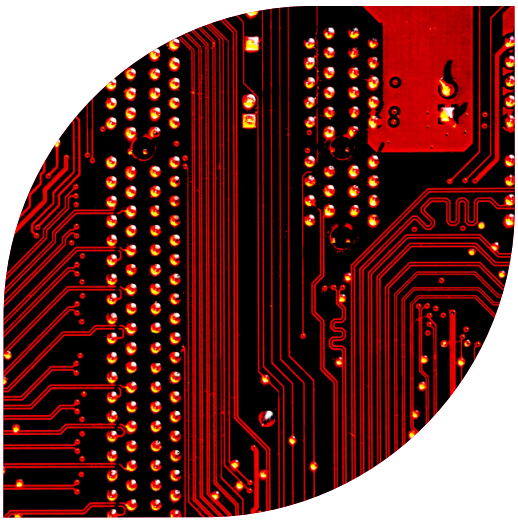
Making sure your business is protected, wherever your team is working

Following the huge increase in people working from home during the pandemic and beyond, more than half of firms believe that their IT systems are now more exposed to attack.

That's the finding from research carried out by the British Chambers of Commerce and Cisco late last year.

They also found:

- One in 10 firms have been the victim of a cyberattack in the last year
- This rises to more than one in seven for larger firms with more than 50 employees
- Only one in five firms have cybersecurity accreditations in place



Shevaun Haviland, Director General at the British Chambers of Commerce, says "The pandemic forced a shift to home working for hundreds of thousands of staff overnight, so it's not surprising firms were caught out by the cybersecurity implications.

"Our research also shows that hybrid working, with many staff splitting their time between the office and home, is here to stay, so it is vital firms have the right cybersecurity protections in place.

"With one in 10 firms confirming they have come under attack in the last year, the need to take action could not be more important."

Aine Rogers, Director of Small Business, Cisco UK & Ireland, says " Organisations are no longer just protecting an 'office' but a workforce at the kitchen table.

"As businesses and individuals, we're more exposed than ever to security threats. That's why we need to evolve thinking to focus on securing your employees and what they are doing, not where they are."

Cybersecurity is hugely important for all businesses – but can feel overwhelming to all except the most technologically-aware.

We're pleased to present a practical, five-point guide to help you protect your IT systems in this most threatening of times.

British Chambers of Commerce | CISCO

5 Cybersecurity Tools to Empower Your Business

Traditionally, technology has served as the foundation for data protection. Yet, as cyber threats continue to evolve, so do the tools businesses need to prevent them. Antivirus software and differentiated passwords are an excellent start but hardly cover the sophistication necessary to properly secure business data today.

So how do you protect your business's data? Here we offer a run-down of the best elements to secure businesses today.

1
Securing your Network Using Firewalls - or Next Generation Firewalls - with Intrusion Protection System

These are often the first line of defence for most organisations, and rightfully so, they're easy to adopt and implement, with little impact on daily operation.

The best firewall solutions for small businesses here:

- Put up a barrier between your trusted internal network and untrusted outside networks, such as the internet
- Control access to your company's resources and prevent the loss of company data
- Prevent disruption of business-critical applications and services due to security breaches

2
Protecting all network communications DNS (Domain Name System) protection

While firewalls may be the first line of defence for networks touching the internet, DNS protection is the first line of defence for all network communications that interact with your business, even from the firewall.

Good DNS protection here:

- Allows speakers in a network conversation to ensure they are not communicating with a bad actor or a network target that has been hijacked or redirected (this is one of the easiest ways to steal data and is normally something a firewall will never see)
- Defends clients from speaking to malware sites, malvertising links and ransomware sites
- Provides protection from 'questionable' sites that may be using an IP address being seen for the very first time on the internet

3
Protecting employees' devices Endpoint protection

Laptops and mobiles are the most vulnerable endpoints for small businesses. The average time to respond to a cyberattack for smaller businesses has increased, not decreased. As malware becomes more evasive, traditional antivirus protection falls short in protecting your endpoints.

The best endpoint security here:

- Works to actively uncover advanced threats like malware and ransomware
- Allows administrators to approve which mobile devices, laptops or desktops can access the network
- Quickly stops threats from spreading and provides fast-track remediation

4
Protecting employees' email Email Gateway Security

Customers of all business sizes face the same daunting challenge: email is simultaneously the most important business communication tool and the leading attack vector for security breaches. It only takes one inadvertent click to bypass a security solution that may have cost millions to acquire and deploy.

The key to a good email security solution is here:

- Detect and prevent access to embedded code, malicious URLs, phishing and fraudulent emails
- User training - a critical element of safe email use - a chain is only as strong as its weakest link. A business's security posture relies on the training and awareness of the humans that use its assets

5
Securing quickly and cost-effectively Cloud-based security

By transitioning data to the cloud, small businesses can tap into enterprise-grade security solutions without having to onboard their own internal teams and infrastructure.

- Cloud-based solutions involve no hardware or software, so they can be quickly and easily deployed, normally for far less expense than hosting the system yourself
- Cloud-based solutions are not immune to attack, so it's important to consider requesting the maximum protection level the cloud provider has to offer
- Regulations may sometimes cause challenges when using cloud storage, so make sure the storage is considered 'compliant' before signing anything

To learn more about these and other cybersecurity solutions for your growing business, visit Cisco's Small Business Security Resources page here.

British Chambers of Commerce | CISCO

Your security experience simplified

Cisco helps organisations who may be feeling overwhelmed about security threats and the associated costs. It's our aim to help you become empowered. With Cisco, you can be confident that your security is in order so you can concentrate on driving your organisation forwards.

- Protect your users everywhere they go
- Free up your team for what's most important
- Consolidate without compromise
- Compliance made easier
- Frictionless security for your employees

Security that works as fast as you do

Things happen quickly in small businesses, so Cisco designed their security to match. With Cisco's threat intelligence, you'll receive protection for previously unknown threats in under 10 minutes – the fastest time to remediation in the industry.

- Leverage the unrivalled breath of intelligence form Cisco Talos
- Separate critical incidents from the noise, so you can act on what's important
- Update policies and implement new capabilities with just a few clicks

Security that grows with your business

Security should limit threats, not your business. Cisco security helps you breathe easier. As your business grows and takes on new challenges, you won't have to keep changing your security strategy every six months.

Take full advantage of the resources and expertise that Cisco includes in their products, to take your business to new heights.

- Manage risk more efficiently as you grow
- Stay one step ahead with Talos threat intelligence that anticipates what's next
- Invest with confidence in security that's designed for the future of working.

For more information on security advice for small businesses visit cisco.com

British Chambers of Commerce | CISCO

BRITISH CHAMBERS OF COMMERCE
65 PETTY FRANCE
LONDON, SW1H 9EU
UNITED KINGDOM

T +44 (0)20 7654 5800
@britishchambers
www.britishchambers.org.uk