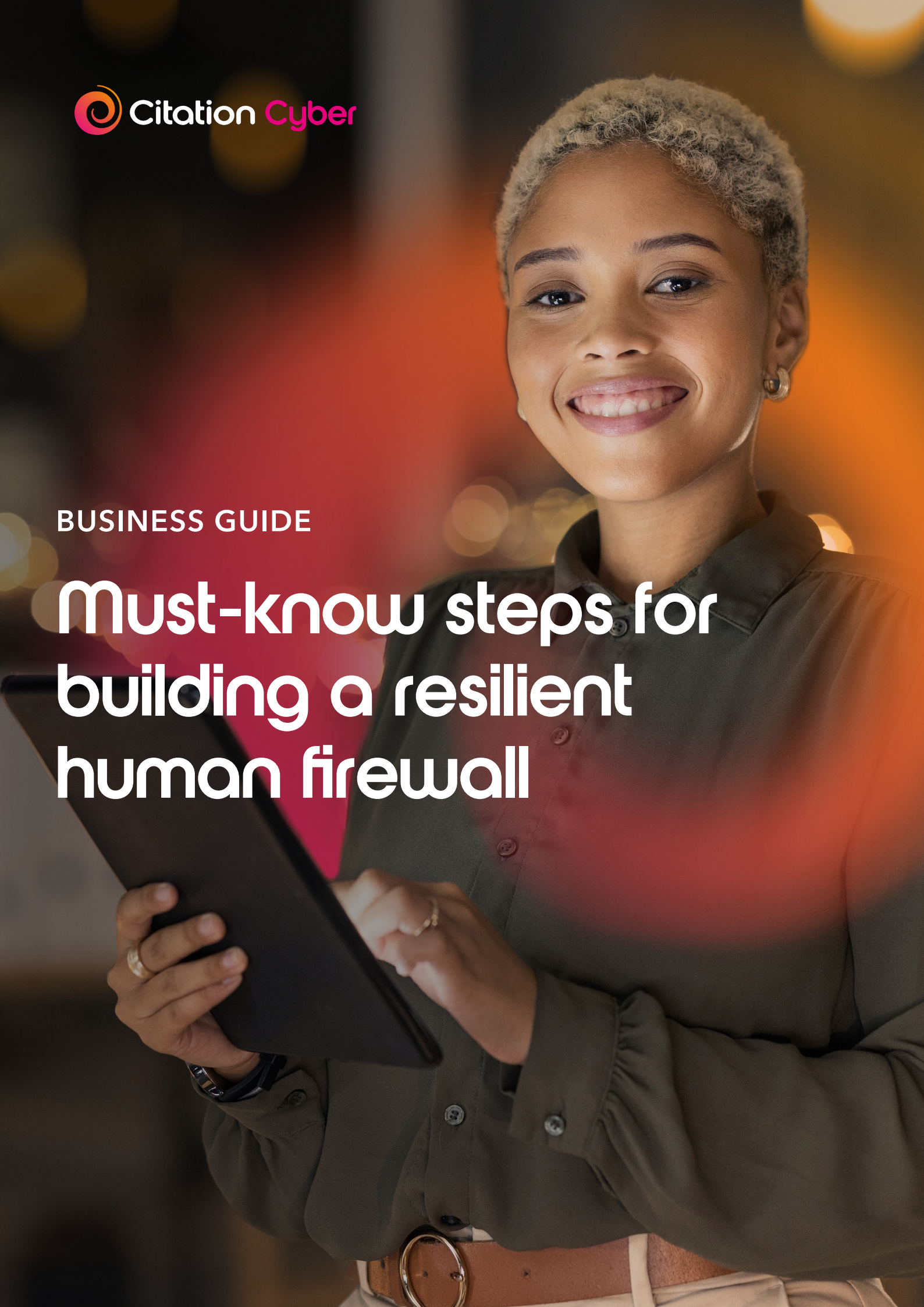
Citation Cyber



BUSINESS GUIDE

Must-know steps for building a resilient human firewall

Introduction

In today's digital world, it's essential to prioritise cyber security. Security threats can come from many different angles; however, it was reported that 74% of data breaches involved a human element (Verizon DBIR 2023).

Social engineering tactics that aim to disarm your human firewall are the most common initial attack vectors when it comes to compromising your business. Therefore, ensuring your workforce is equipped with the knowledge and skills to defend against cyber criminal activity is a crucial step in protecting your business.

Cyber security is a critical concen for organisations of all sizes and industries. But how big is the threat to UK businesses today?

In this guide, we'll look at the key steps to increasing empowerment throughout your organisation, and how taking some relatively simple steps can potentially save your business.

The threat landscape

83%

of organisations have suffered from more than one security breach

UK

is the most cyber attacked country in Europe, accounting for 43% of cases

60%

of cyber breaches in Europe involve social engineering tactics

74%

of breaches involve the human element

41%

of incidents involve phishing for initial access

19%

of breaches are caused by stolen credentials

Understanding the power of cyber awareness and culture

If you and your business perform regular penetration testing of your systems and networks, then this is an extremely beneficial step in keeping your devices and data secure.

However, this is not a be-all-end-all solution. A business can spend thousands on annual testing, but ultimately, it only takes one click of the wrong link sent in a phishing email to make all these efforts redundant.

Cyber security isn't solely about ensuring your network and devices are secure, it's about ensuring the individuals who are using these networks and devices and secure too!

Cyber security empowerment is the process of enabling your employees at all levels of the organisation to be accountable and take ownership of cyber security measures.

It involves equipping employees with the knowledge, skills, and resources to identify and mitigate cyber security risks, and encourage a culture of security awareness and best practices.

FIND OUT MORE →

The secrets . . .

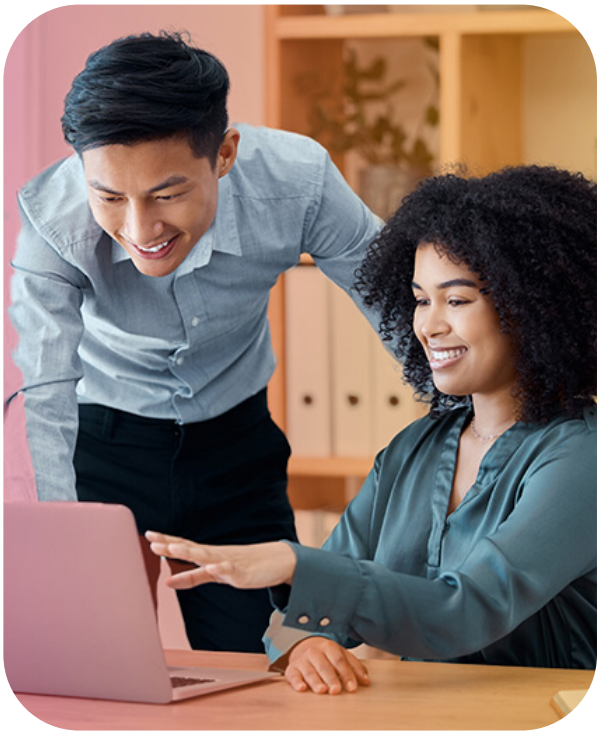
Lead by example

Leadership plays a crucial role in empowering employees to prioritise cyber security. Leaders in the workplace need to lead by example and demonstrate a strong commitment to cyber security best practices.

It is imperative to regularly communicate the importance of cyber security, follow established protocols themselves, and hold employees accountable for their cyber security responsibilities.

Interactive, meaningful training

Education and training are vital to empower employees with the knowledge and skills to identify and respond to cyber security threats. Businesses should look to offer regular cyber security awareness training to all employees (regardless of their roles and responsibilities) as an effort to build their security resilience.



It is important to not let these training session be a tick-box exercise! Providing ongoing education and resources to help keep your team updated on the latest cyber threats and best practices is key.

Security permissions

Appropriate access controls and permissions are critical to limit the risk of unauthorised access to sensitive data and systems.

Review and update access control policies and permissions regularly, based on the principle of the least privilege.

Empower employees with the necessary permissions to perform their job responsibilities, whilst restricting access to sensitive information or systems that are not relevant to their roles.

Encourage Transparency

It is crucial for organisations to promote an honest and proactive incident reporting throughout the workplace.

Those who punish employees for errors could result in individuals hiding these mistakes, leading to further damage later down the line. Increase awareness and provide clear guidelines and channels for employees to promptly report any suspected, or genuine, cyber security incidents.

Establish an incident response plan that outlines the steps to be taken in case of a security breach and empower employees to take appropriate actions to mitigate an incident.

Make cyber security a priority

Implementing cyber security throughout your organisation will enforce healthy security behaviours amongst your workforce.

By making cyber security a priority in your business, you will demonstrate to your team, clients, and stakeholders that you take the protection of their devices and data seriously.

Having regular conversations, training, and awareness about cyber security will help keep this front of mind and reiterate its importance in our ever-evolving digital world.

Benefits of awareness training

- Training your employees helps reduce human errors that can result in a security breach, enhancing your organisation's overall security.
- Cyber attacks can cause significant disruptions. Effective training can prevent attacks and the subsequent downtime they cause.
- Employee training fortifies how an organisation protects their sensitive data, helping to build and maintain client trust.
- Data breaches can result in huge organisation fines. Awareness training provides an additional layer of defence against cyber breaches.
- Security training is an effective way of communicating regulatory responsibilities to your staff and ensuring they follow the necessary codes of compliance.
- Awareness training is a low-cost, yet extremely effective way of reduce your risk of a cyber breach by up to 80%!

The ultimate solution for your business

Do you want to become cyber secure? With our on-going cyber security support, you can! We'll train, test, and certify your business to minimise data breaches and cyber attacks.

Our solutions are designed to help you become a business that your clients can trust, and what's more is that you'll remain compliant, win more tenders, and improve your overall efficiency. Watch your business soar when you're cyber secure!

Let's make securing your business just that much easier. We cut the faff, the jargon, and keep cyber security as it should be . . . simple!

All our packages can be tailored to meet your specific business requirements, so we recommend kicking things off with a free business needs assessments and software demonstration.

Book today by clicking here or calling our friendly team on 0333 323 3981.

As a flavour of the support we offer, our entry-level 'Secure Core' package includes:

- Cyber Essentials certification
- Guidance and technical support with your Cyber Essentials assessment
- £25k cyber insurance
- 2x External vulnerability scans
- Dark web monitoring
- Cyber security awareness course for your team
- 12x cyber policy templates
- HR advice line
- Free employee screening registration
- Access to the state-of-the-art user hub where you can manage your security solutions, store your company policies, and monitor your training strategy.

FIND OUT MORE →

And for those wanting complete cover, we've got our all-in-one 'Secure Pro' including dedicated compliance training modules, and external intelligent monitoring and vulnerability scanning.

Got any questions or ready to get the ball rolling? Call **0333 323 3981** or email us at **info@citationcyber.com**

Watch your business soar when you're cyber secure!

Got any questions or ready to get the ball rolling? Call **0333 323 3981** or email us at **info@citationcyber.com**

Citation Cyber