NAVIGATING THE CYBER SECURITY LANDSCAPE

A guide for property firms looking to shield their business from cyber threats

acora ONE

The evolving cyber security landscape & the property sector

The property sector in the UK faces a growing cyber threat. Firms in this industry handle sensitive client data, making them attractive targets for cyber criminals.

The property sector forms an important part of the UK economy. As of early 2023, there were over 114k enterprises in total including Estate Agents, Property Development, and Sourcing companies operating in the UK, with an estimated total revenue of £65B (ONS). Total value of all UK property reached £8.68T (Savills).

This financial scale not only highlights the property sector's vital role but also emphasises the need for heightened vigilance and robust measures to protect both the sector's economic contributions and the confidential information entrusted to it.

KEY CYBER SECURITY CHALLENGES FACING THE PROPERTY SECTOR

The property sector is increasingly targeted by cyber criminals, facing significant challenges in protecting sensitive client information and maintaining robust digital security.

1

Data Protection & Privacy

Protecting your clients' personal data is a critical aspect of your business operations.

As you handle sensitive client information daily, from financial details to personal contacts, ensuring robust data protection and privacy is crucial. The shift to digital record-keeping and transactions heightens the risk of potential data breaches.

A breach can lead to significant legal and financial repercussions, especially under GDPR regulations. Therefore, maintaining the confidentiality and security of client data is not just a cyber security issue but integral to your firm's trust and compliance.

2

Phishing & Social Engineering Attacks

Your business is increasingly vulnerable to phishing and social engineering attacks in the property sector.

These sophisticated attacks often target employees through deceptive emails or communications, aiming to extract sensitive information or redirect financial transactions. The frequent and varied interactions in property dealings make your firm particularly susceptible.

Falling victim to these scams can lead to significant financial losses and breach of client trust. Educating your team to recognise and respond to these threats is essential in safeguarding your business operations and maintaining client confidence.

3

Ransomware & Malware Threats

Ransomware and malware pose a serious threat to the security of your business.

These types of cyber-attacks can cripple your firm’s digital infrastructure, locking access to critical data such as property listings and client databases. The reliance on digital systems for daily operations makes your business a target.

A successful attack can disrupt business continuity, result in data loss, and damage client relations. Implementing robust cyber security measures and regular data backups are vital to protect against these threats and ensure the resilience of your business.

4

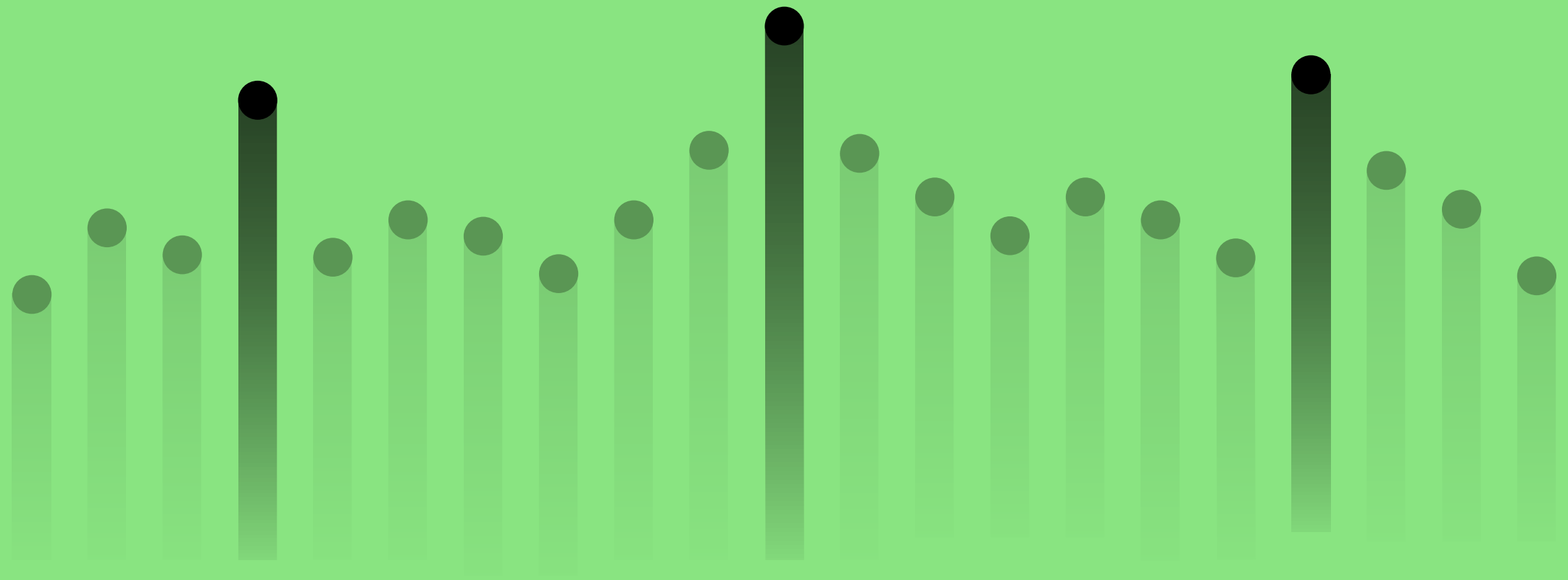
Remote & Network Security

Your organisations shift towards remote work and digital operations heightens the need for robust remote and network security.

With the increasing trend of remote work and online transactions in the property sector, securing remote access to your network and protecting online interactions is imperative. This includes safeguarding against unauthorised access and potential data breaches.

Inadequate remote network security exposes your agency to cyber threats, risking client data and the integrity of transactions. Strengthening security protocols and conducting regular network assessments are crucial steps in safeguarding your firm’s digital environment.

TOP 3 STRATEGIES TO PROTECT YOUR BUSINESS



1

Engaged and informed leadership

It's imperative that the leadership in the business are deeply involved in understanding and guiding your cyber security strategy.

The engagement from the top sets the tone for the entire firm, emphasising the critical nature of cyber security in protecting clients and the business.

Leveraging resources like the NCSC's Cyber Security Toolkit for Boards is vital in this journey. This toolkit is specifically designed to provide you with the knowledge and tools necessary to comprehend and address cyber security risks effectively. It's not just a resource; it's a roadmap that helps bridge the gap between technical jargon and strategic decision-making.

Benefits of engaged and informed leadership

- Enhanced risk management
- Stronger security posture
- Improved compliance
- Fostering a culture of security
- Client confidence and trust

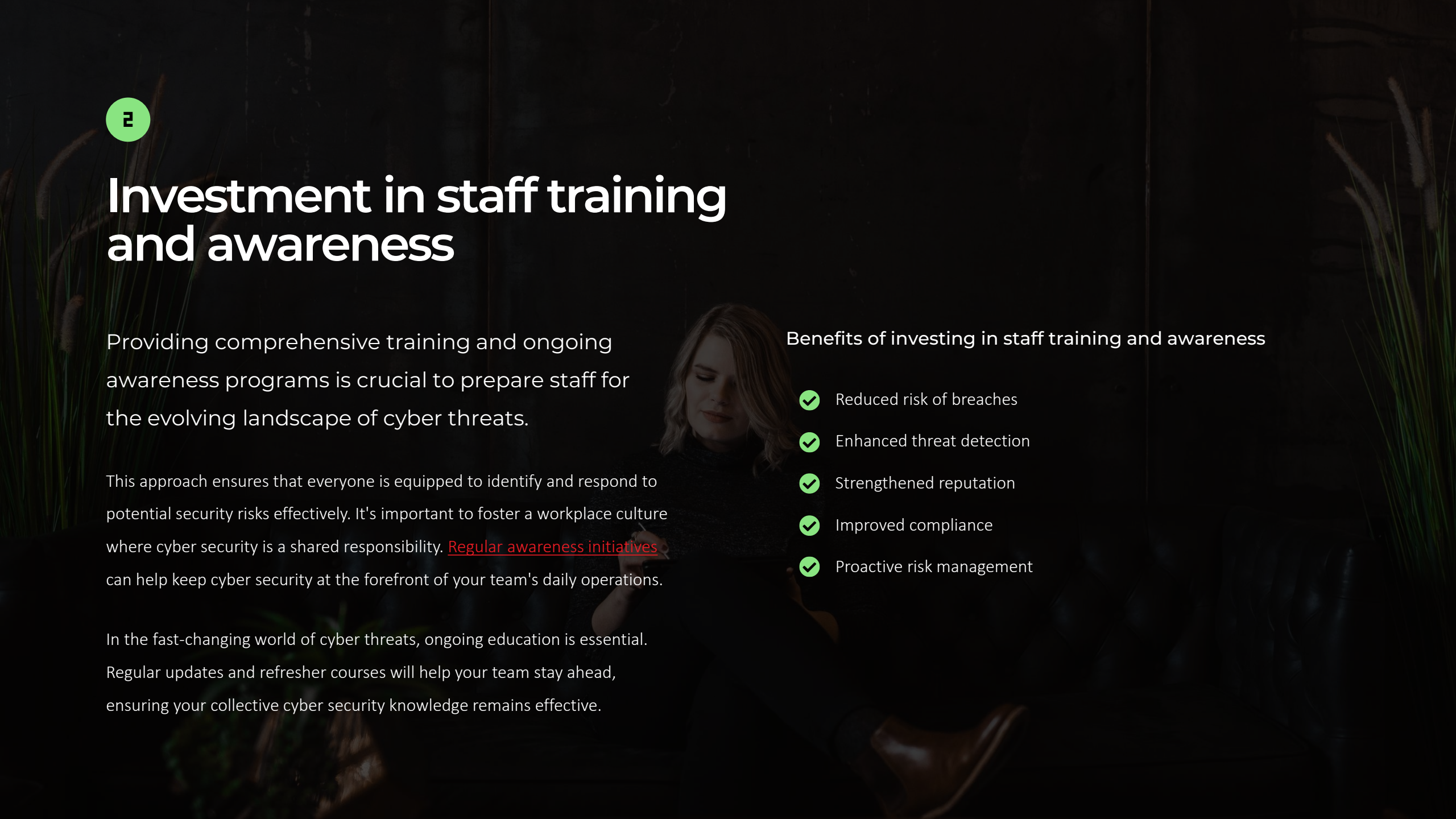
2

Investment in staff training and awareness

Providing comprehensive training and ongoing awareness programs is crucial to prepare staff for the evolving landscape of cyber threats.

This approach ensures that everyone is equipped to identify and respond to potential security risks effectively. It's important to foster a workplace culture where cyber security is a shared responsibility. Regular awareness initiatives can help keep cyber security at the forefront of your team's daily operations.

In the fast-changing world of cyber threats, ongoing education is essential. Regular updates and refresher courses will help your team stay ahead, ensuring your collective cyber security knowledge remains effective.



Benefits of investing in staff training and awareness

- Reduced risk of breaches
- Enhanced threat detection
- Strengthened reputation
- Improved compliance
- Proactive risk management

3

Cyber Essentials certification

Working in the property sector, you understand the importance of safeguarding sensitive client information and maintaining the integrity of operations.

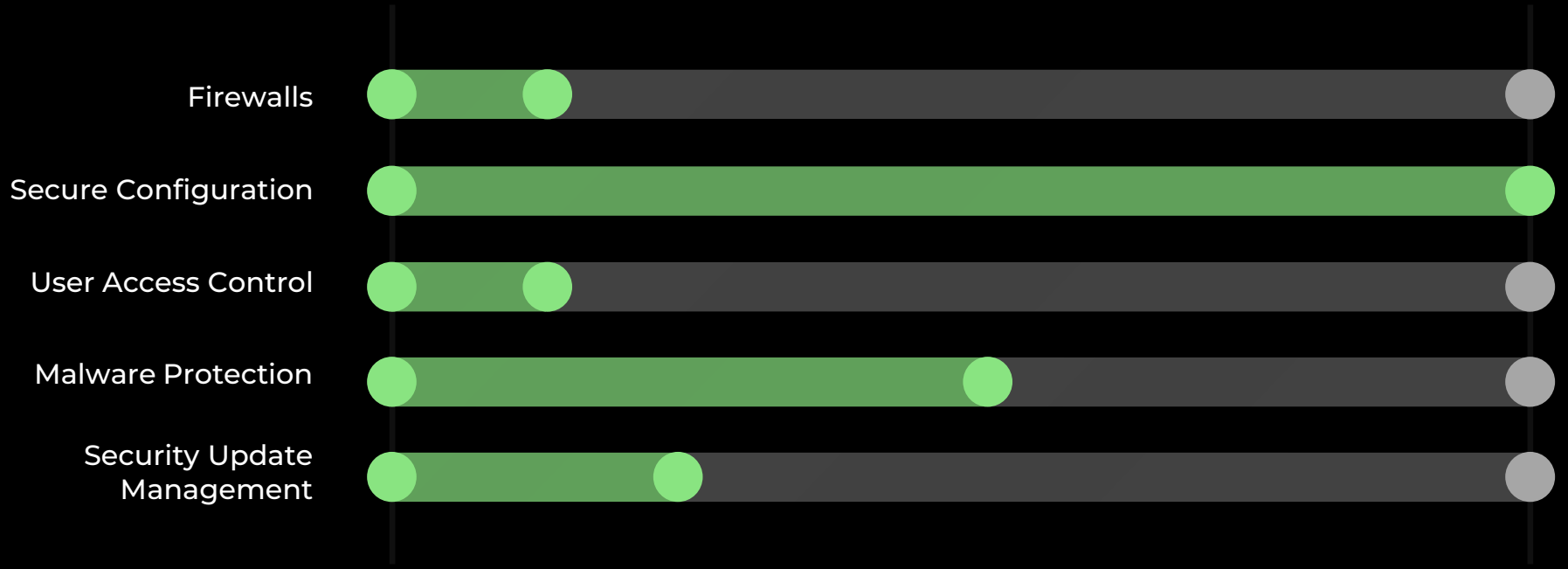
Embracing Cyber Essentials can provide a solid foundation for protecting your business from common online threats and ensuring that you are compliant with regulatory requirements.

Cyber Essentials is a government-backed scheme that's cost-effective, straightforward approach to enhancing cyber security. It consists of 5 technical control themes: Firewalls, Secure Configuration, User Access Control, Malware Protection, and Security Update Management.

Benefits of Cyber Essentials certification

- Enhanced cyber threat protection
- Improved client confidence
- Reduced insurance premiums
- Compliance with contractual requirements
- Strengthened business reputation

Getting Cyber Essentials certified with a Gap Analysis



What are the benefits of a Cyber Essentials Gap Analysis?

- **Identifying security weaknesses** – Identify precise areas where your firm's cyber security practices may not meet the recommended standards. This focused analysis helps you recognise vulnerabilities and implement necessary improvements.
- **Tailored improvement strategies** – Receive custom-tailored improvement recommendations that are invaluable for shaping a targeted strategy to fortify your firm's Cyber Security defences in the most effective manner.
- **Enhancing cyber security readiness** – Addressing the identified gaps enhances your firm's preparedness against prevalent cyber threats, a critical step in an evolving landscape where threats are continually growing in sophistication and frequency.
- **Building client trust and confidence** – Demonstrating that you have conducted a thorough Cyber Essentials Gap Analysis and acted upon its findings reassures clients of your commitment to protecting their sensitive data.
- **Aligning with industry best practices** – Align your cyber security practices with industry-leading standards. This alignment not only enhances client confidence but also positions your business as a responsible and forward-thinking player in the property sector.
- **Preparation for Cyber Essentials certification** – Establish a foundation towards Cyber Essentials certification. Ensure your business meets essential criteria and paves a straightforward path towards acquiring this significant accreditation.

Empower your company with a comprehensive Cyber Essentials Gap Analysis.

Contact us today to schedule a consultation with one of our experts and start protecting your business.

Get in touch


acora
one