NAVIGATING THE CYBER SECURITY LANDSCAPE

A guide for legal practices looking to shield their business from cyber threats

acora ONE

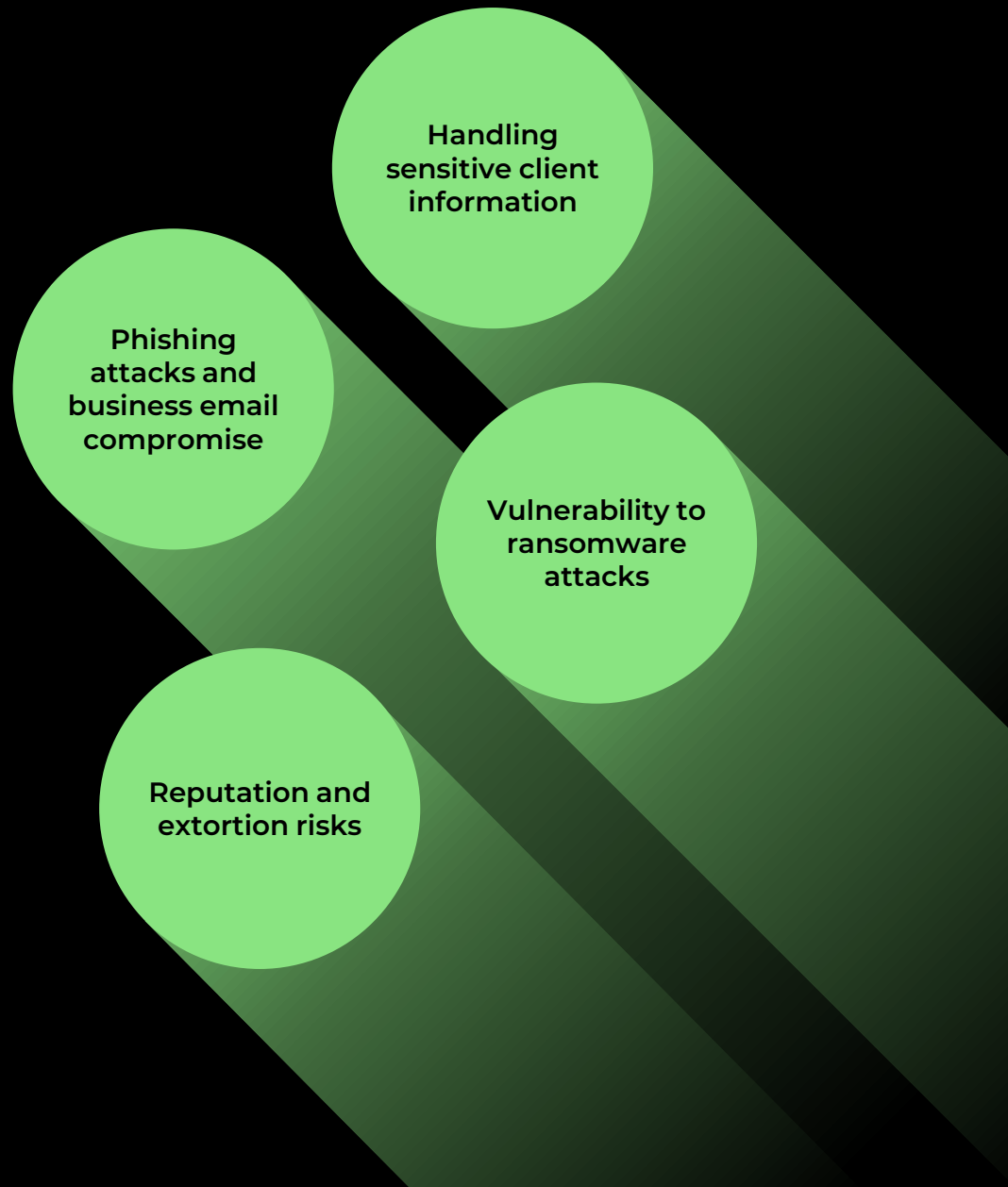
The evolving cyber security landscape & the legal sector

The legal sector in the UK faces a growing cyber threat. Law firms handle sensitive client data, making them attractive targets for cyber criminals.

Legal services form an important component of the UK economy. As of early 2023, there were over 32.9k enterprises in total including barristers, solicitors and other legal service providers operating in the UK, with an estimated total revenue of £43.9B.

The SRA published 278 scam alerts in response to reports from the public and profession between January 2022 and January 2023. These scam alerts highlight reports of people falsely claiming to be solicitors and firms, for example on websites or in emails and telephone calls.

KEY CYBER SECURITY CHALLENGES FACING THE LEGAL SECTOR



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

1

Handling sensitive client information

Handling sensitive client data is a daily task, encompassing everything from personal affairs to corporate dealings.

The digitisation of these processes, while efficient, heightens the risk of cyber breaches. Your challenge is to ensure robust digital security, where even a single vulnerability can lead to significant data exposure, undermining the confidentiality essential to your client relationships.

As a result, a breach in client data security has far-reaching implications. For your clients, it could mean financial loss or compromised legal positions. For your business, the repercussions extend to enduring reputational damage, loss of client trust, and potential legal liabilities.

2

Vulnerability to ransomware attacks

As a legal practice, you're increasingly at risk of ransomware attacks, a pressing cyber security threat.

The challenge lies in fortifying your IT infrastructure against such attacks, which requires both technological solutions and staff vigilance. Failing to do so could lead to paralysing your operations and jeopardising sensitive client cases.

The impact of a successful ransomware attack on your business can be devastating. Operational disruptions can result in significant loss of billable hours and client service delays, directly affecting your bottom line. Moreover, there's the reputational damage to consider. Ransomware incidents can severely erode this, potentially leading to long-term client loss and damage to your firm's reputation.

3

Phishing attacks & Business Email Compromise (BEC)

Phishing attacks and Business Email Compromise (BEC) are critical threats in your sector.

These attacks aim to manipulate staff into transferring funds or revealing sensitive information. Given the nature of legal transactions and the large sums involved, your practice is particularly vulnerable. The challenge is to enhance email security and educate your team to recognise and respond appropriately to these deceptive tactics, safeguarding against financial and data losses.

Financially, these attacks can lead to significant monetary losses, either through direct theft or by compromising client transactions. Additionally, there's the risk of confidential information being exposed.

4

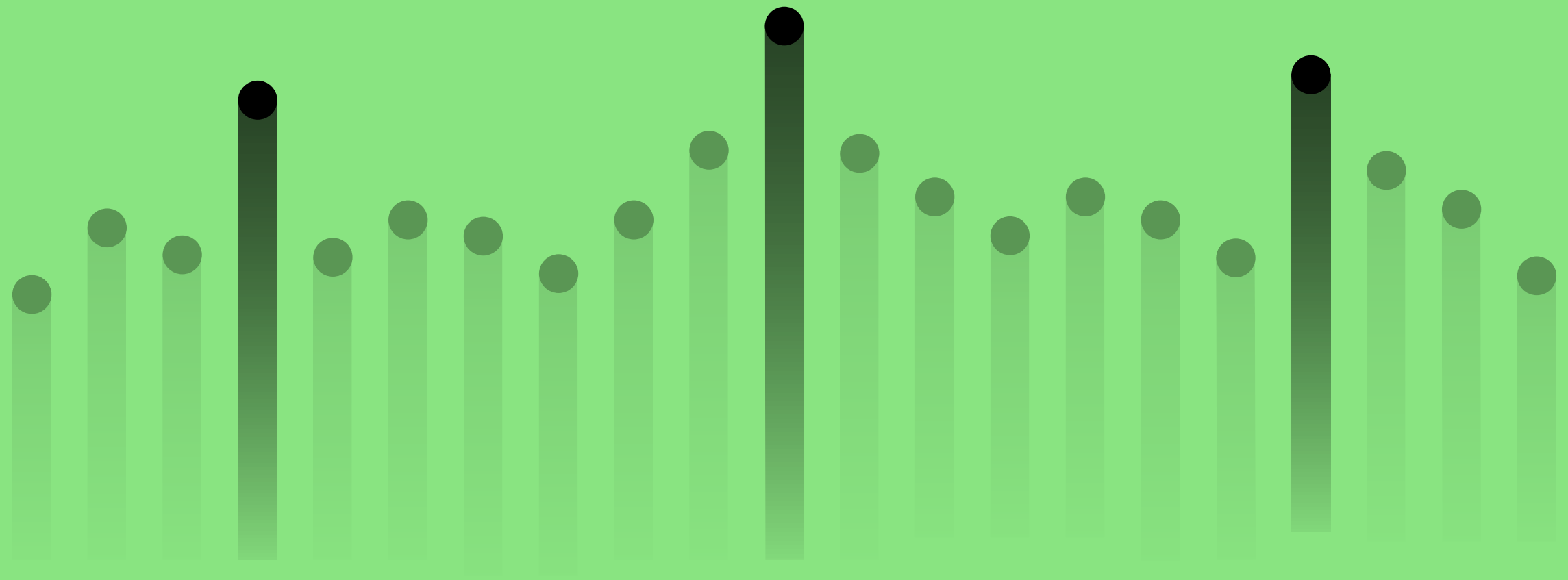
Reputation and extortion risks

Your firm's reputation is paramount and closely tied to client trust.

This makes you a prime target for extortion threats, such as ransomware or doxxing, where attackers threaten to release sensitive data unless demands are met. The key challenge is not just technical defence against such attacks, but also preparing a strategic response plan that includes communication and legal considerations.

If a ransom is paid or the attack averted, the mere suggestion of compromised client data can irreparably damage your firm's reputation. There's a real risk of legal and regulatory repercussions too, particularly if client data is involved.

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

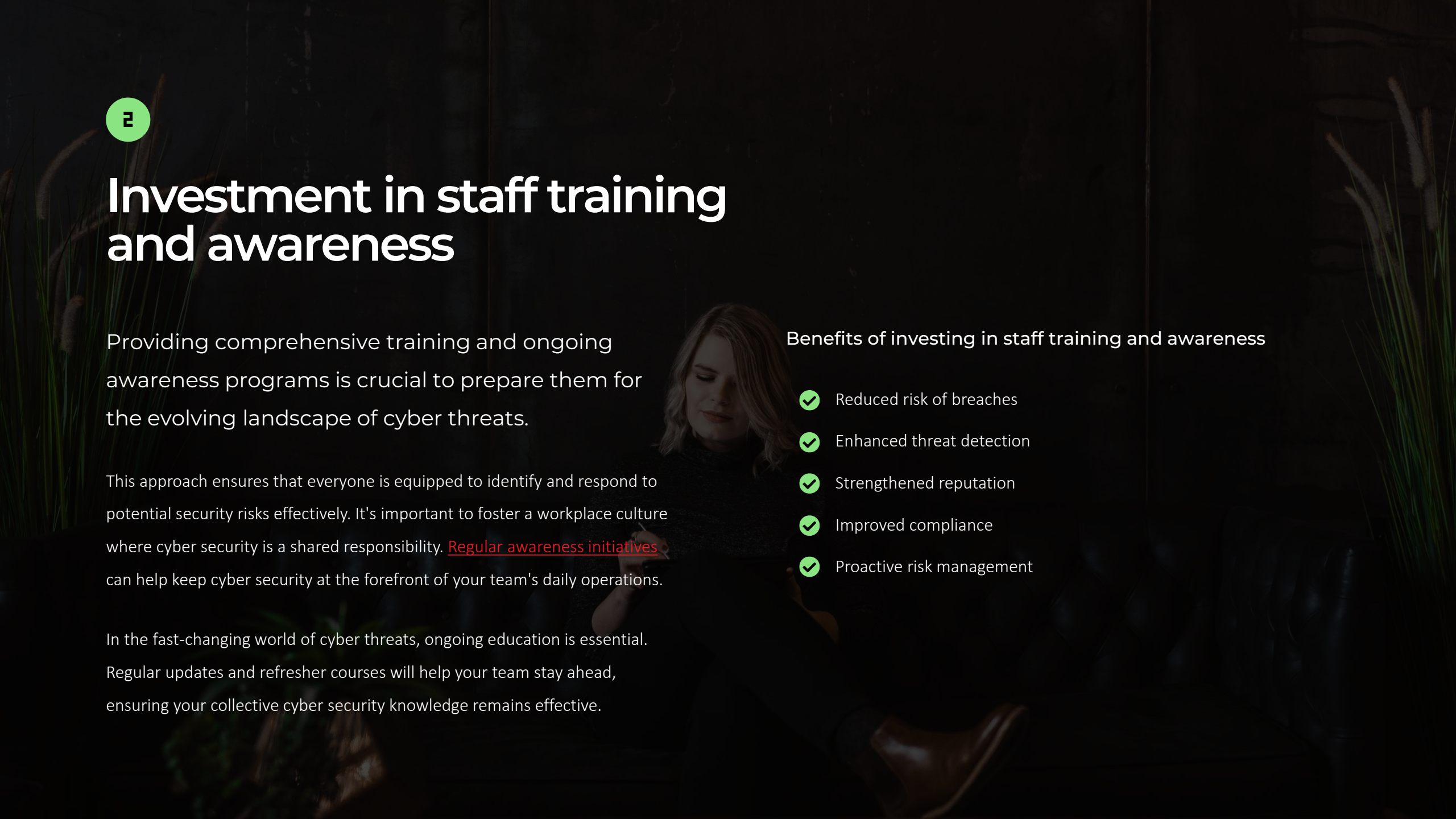
2

Investment in staff training and awareness

Providing comprehensive training and ongoing awareness programs is crucial to prepare them 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

As a legal partner, you understand the importance of safeguarding sensitive client information and maintaining the integrity of your firm's operations.

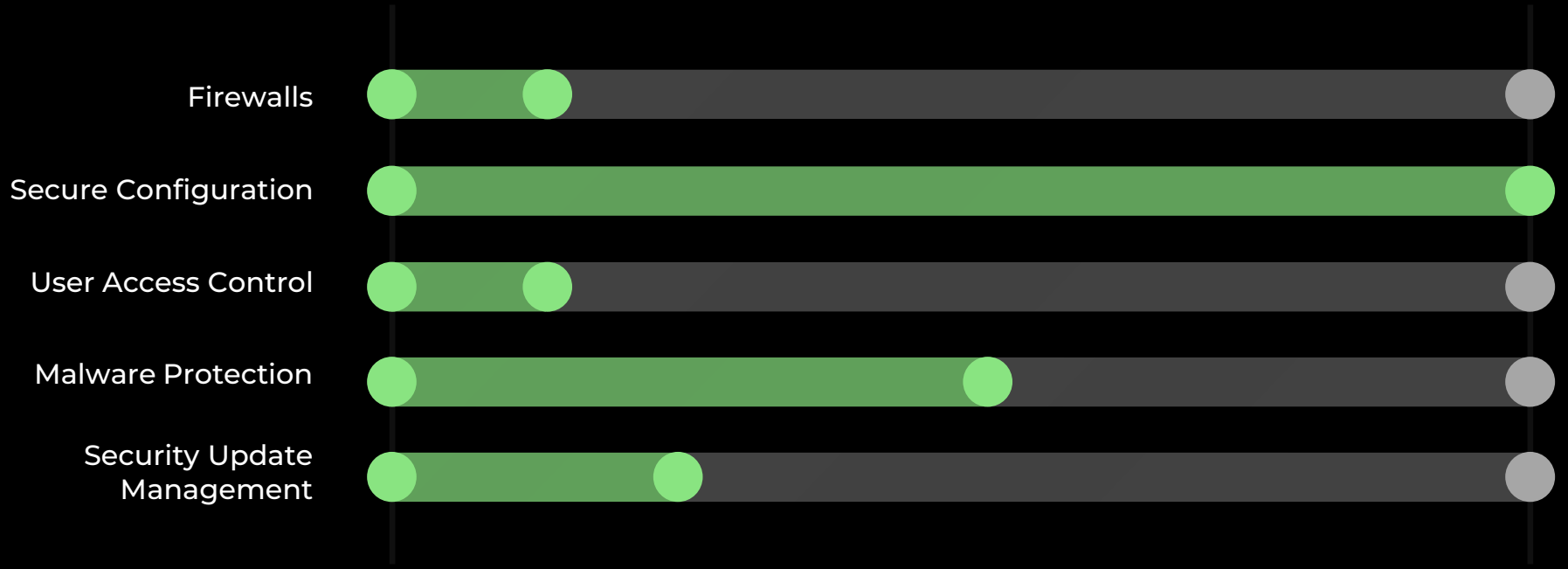
Embracing Cyber Essentials can provide a solid foundation for protecting your business from common online threats and ensuring that you are compliant with regulatory requirements.

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** – Pinpoint specific areas where your firm's cyber security measures may not align with the recommended standards. This targeted insight allows you to understand your vulnerabilities and take corrective action.
- **Tailored improvement strategies** – It offers tailored recommendations for improvement. This guidance is invaluable in developing a focused strategy to enhance your cyber security defences in the most effective way.
- **Enhancing cyber security readiness** – By addressing the gaps identified, your firm strengthens its readiness against common cyber threats. This is crucial in a landscape where threats are constantly evolving and becoming more sophisticated.
- **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 best practices. This alignment is not only beneficial for client assurance but also positions your firm as a responsible and forward-thinking entity in the legal sector.
- **Preparation for Cyber Essentials certification** – Create a stepping stone towards achieving Cyber Essentials certification. It prepares your firm by ensuring that you meet the necessary criteria, setting a clear path for obtaining this important certification.

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