NAVIGATING THE CYBER SECURITY LANDSCAPE

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

acora ONE

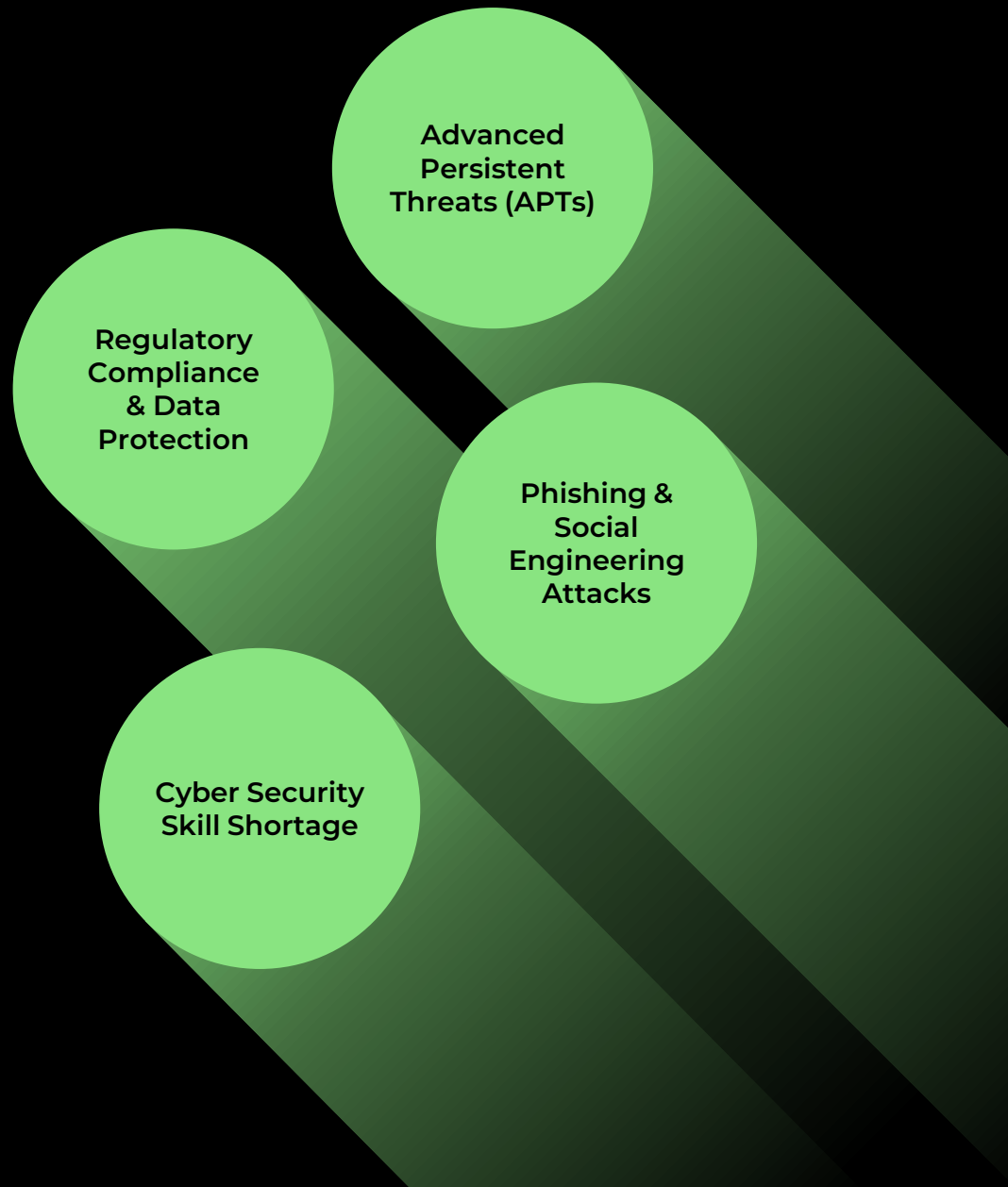
The evolving cyber security landscape & the finance sector

The finance 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 financial and professional services (FPS) industry is the engine room driving UK growth. With 2.5 million people employed across the UK – over 1.1 million in financial services and more than 1.3 million in related professional services – the industry produced £278bn of economic output, 12% of the entire UK's output (HM Treasury).

This financial magnitude not only underscores the finance sector's critical role but also underscores the necessity for increased vigilance and strong safeguards to preserve both the sector's economic significance and the sensitive information it holds.

KEY CYBER SECURITY CHALLENGES FACING THE FINANCE SECTOR



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

1

Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) present a formidable challenge in the finance sector, characterised by their stealthy, sophisticated, and long-term nature.

These attacks involve highly skilled adversaries who gain unauthorised access to financial networks, maintaining a foothold for prolonged periods to extract sensitive data. The complexity of these threats often evades conventional security measures, making early detection and response difficult.

The persistent nature of APTs requires financial institutions to employ advanced security strategies, including real-time monitoring, AI-driven threat detection, and continuous employee training.

2

Phishing & Social Engineering Attacks

Phishing and social engineering attacks represent a significant cyber security challenge for the finance sector, exploiting human vulnerabilities to breach security.

These tactics deceive employees into revealing sensitive information or granting access to secure systems, bypassing traditional cyber security measures. The sophistication of these attacks, often tailored and highly convincing.

Addressing this challenge involves comprehensive employee training and awareness programs, alongside robust verification protocols. Financial institutions must foster a culture of security awareness, where staff are equipped to recognise and respond to these deceptive techniques.

3

Regulatory Compliance & Data Protection

Regulatory compliance and data protection pose a complex challenge for the finance sector, requiring adherence to a dynamic landscape of legal and regulatory requirements.

Financial institutions must navigate and implement policies in line with evolving regulations like GDPR, often involving significant changes to data handling and processing practices. This task is complicated by varying international standards and the need for continuous adaptation.

Overcoming this challenge demands a proactive approach, with regular training for staff, comprehensive audits, and investment in systems capable of ensuring compliance.

4

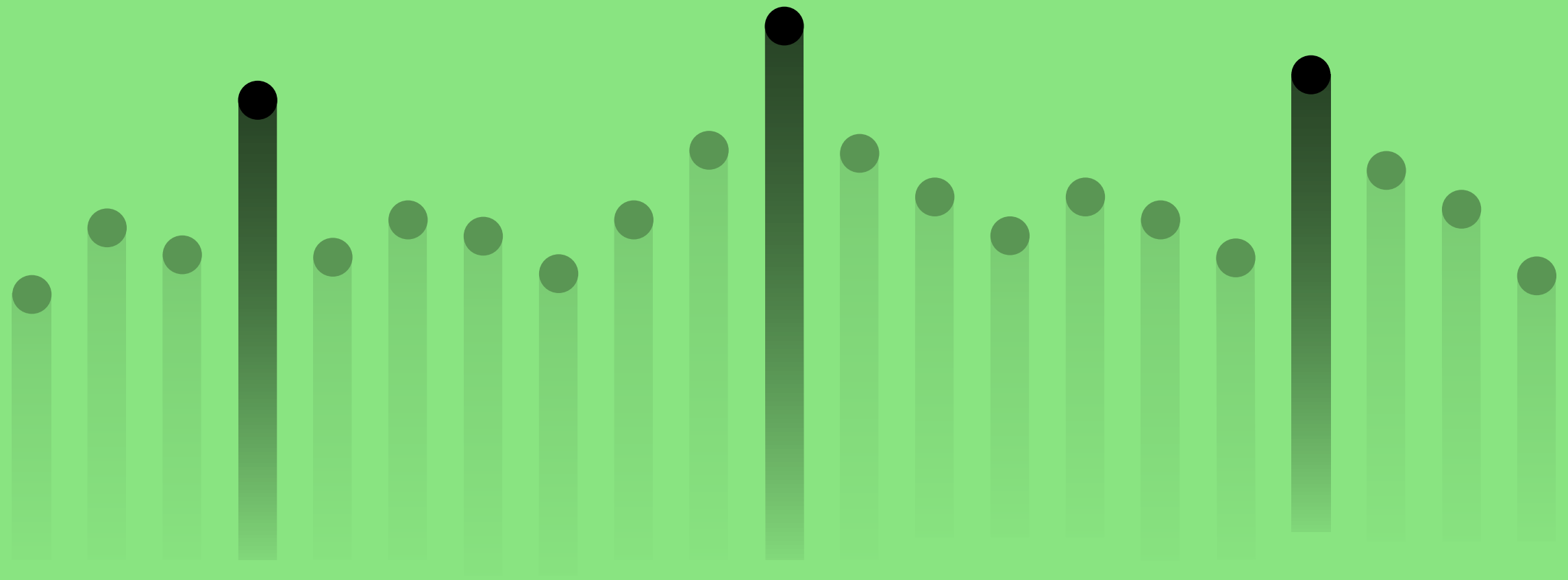
Cyber Security Skill Shortage

The cyber security skill shortage presents a critical challenge for the finance sector, impacting its ability to effectively combat evolving cyber threats.

This gap is marked by a scarcity of qualified cybersecurity professionals, hindering the development and implementation of robust security strategies. The rapid advancement of cyber threats outpaces the available expertise in many financial institutions.

To address this issue, the sector must focus on nurturing talent through dedicated training programmes, partnerships with educational institutions, and embracing innovative technologies like AI for security automation. Investing in skill development and adopting new approaches are key to mitigating the risks.

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

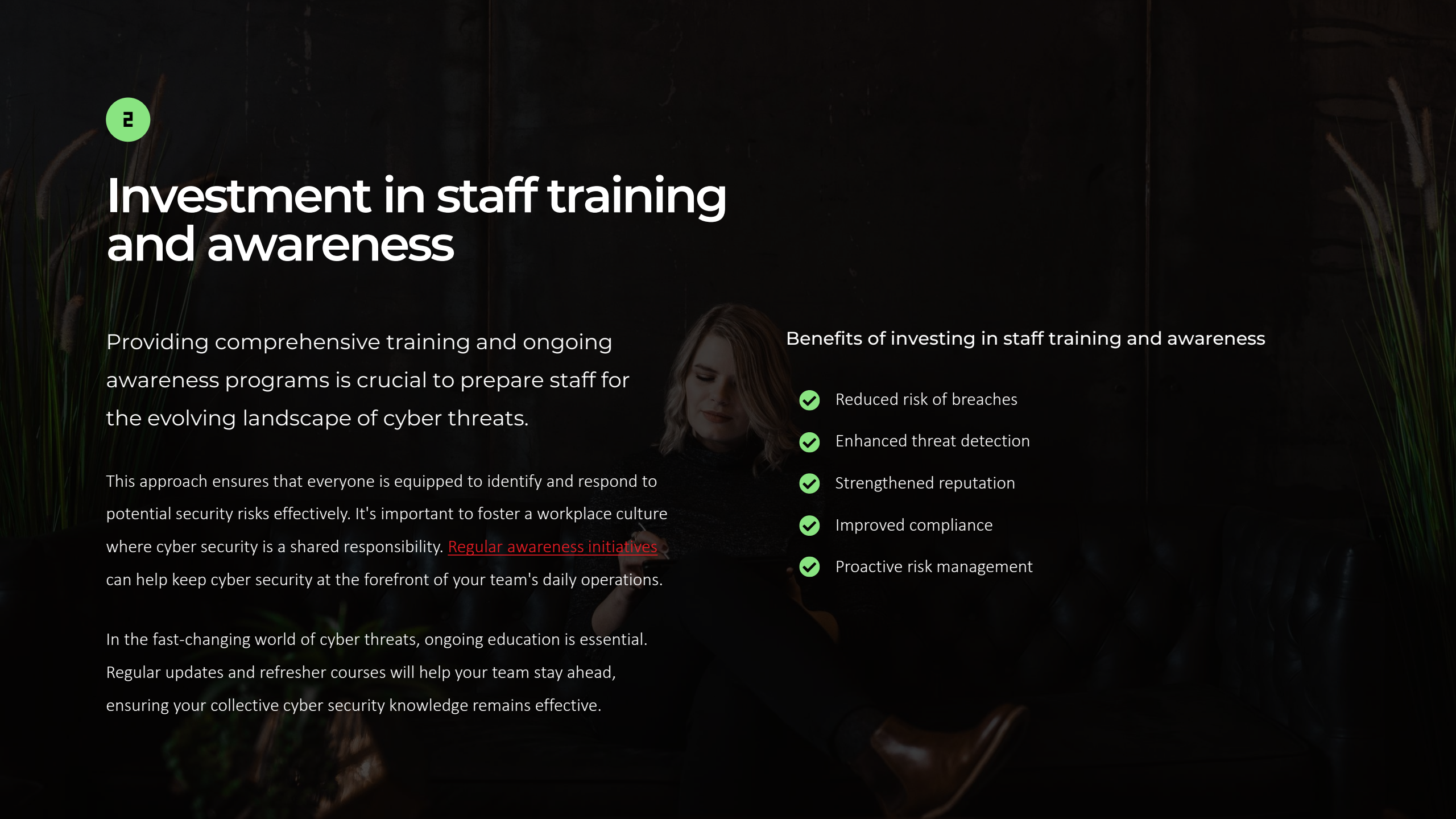
2

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

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

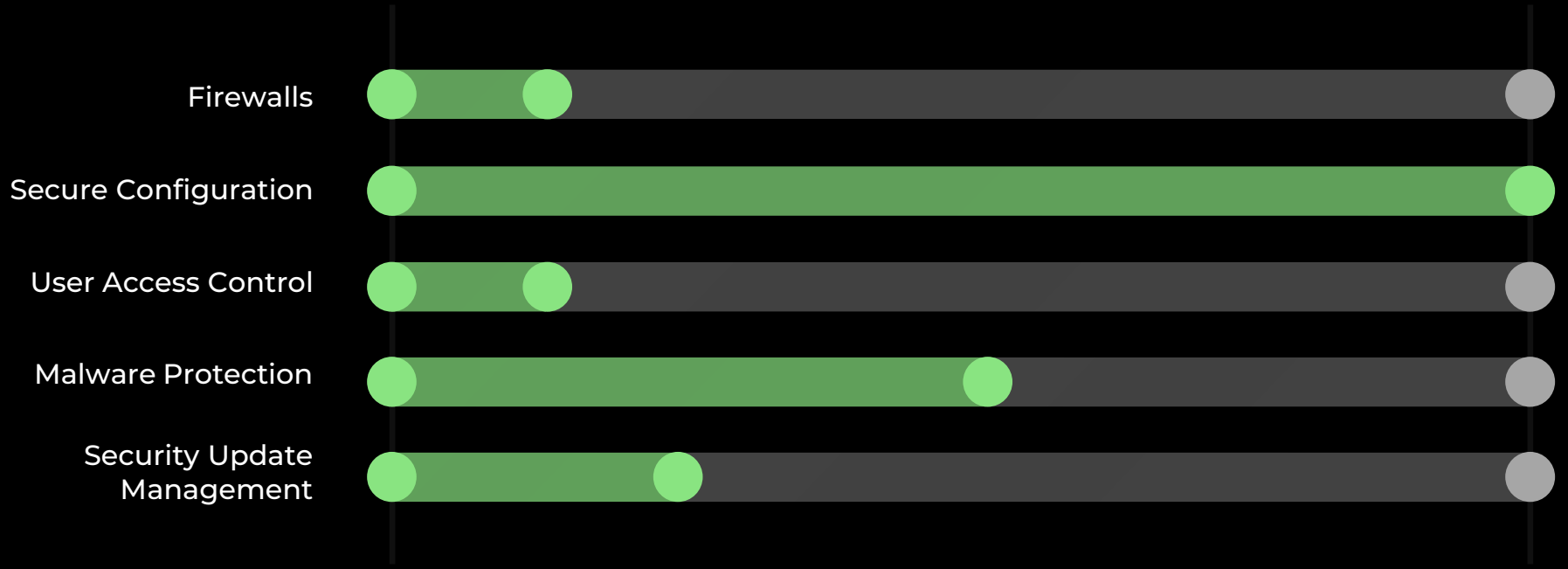
Embracing Cyber Essentials can provide a solid foundation for protecting your business from common online threats and ensuring that you are compliant with regulatory requirements.

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** – 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 agency'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 firm as a responsible and forward-thinking player in the finance sector.
- **Preparation for Cyber Essentials certification** – Establish a foundation towards Cyber Essentials certification. Ensure your firm 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