Bright

Simply brilliant software

Guide to Cybersecurity and Data Protection

Businesses across the UK are under increasing threat from cybercrime and fraud, with **39% of businesses reporting cyberattacks or security breaches in the past year**. These incidents cause real damage, with the average cost of a data breach or cyberattack sitting at **£5,500** – a figure that increases the larger the business. In total, cybercrime cost businesses £30.5 billion in 2023.

IMost worryingly is the news that small businesses are making up an ever-larger share of the companies targeted. In 2023, small businesses employing between 11 and 50 people showed the steepest rise in targeting among all companies surveyed, up 42% since 2019. However, much of the damage is avoidable.

According to a report by GCHQ, many attacks could be deflected by improving basic *"cyber hygiene"*. Even today, many companies fail to implement essential steps such as multi-factor authentication, strong passwords or basic system updates.

As the threats against businesses mount, it will fall to accountants to take a leading role in safeguarding their clients' financial data and keeping their practices safe.

Bright

The basics of cybersecurity

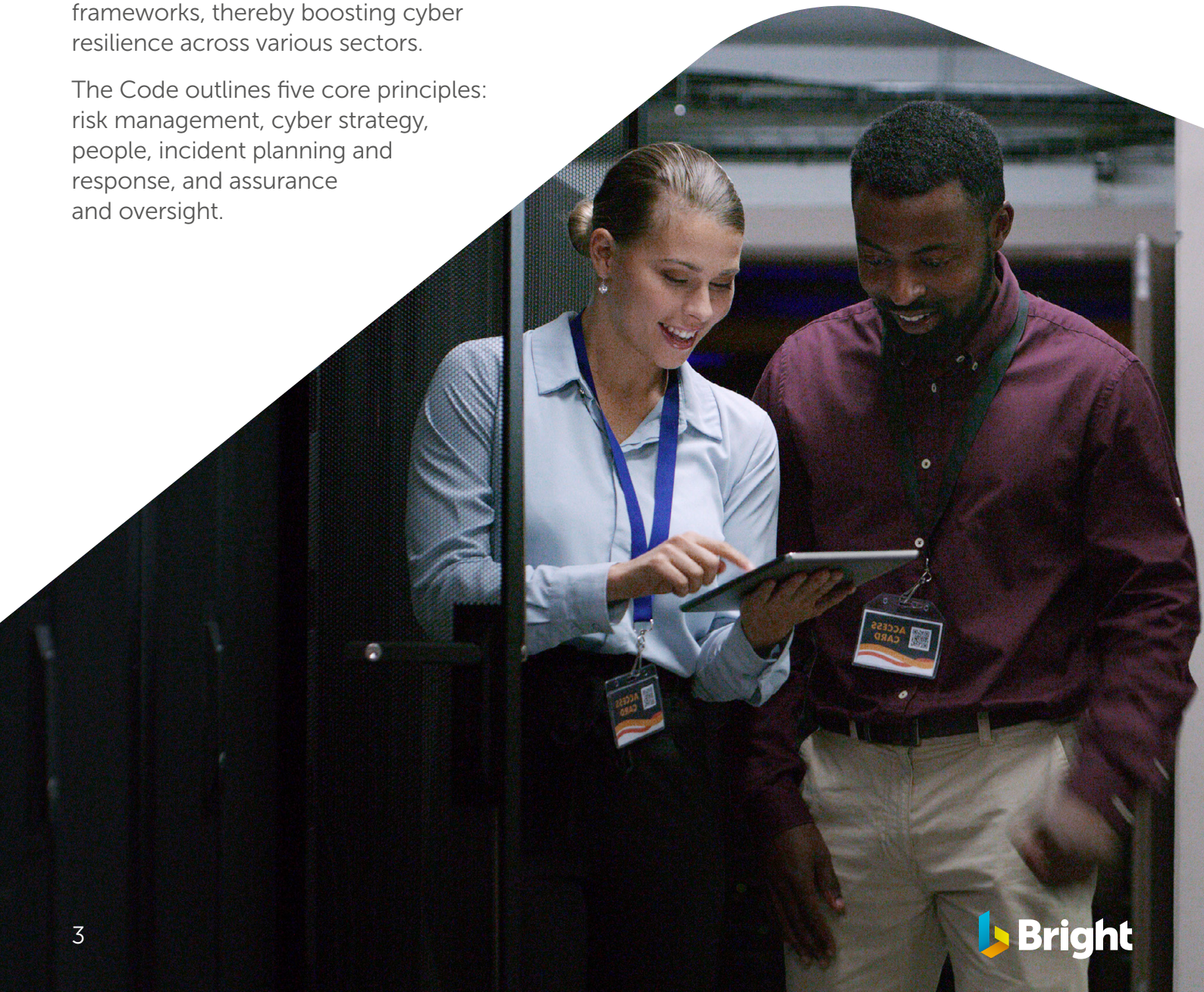
As guardians of sensitive and valuable financial data, professional services are more vulnerable than most businesses when it comes to cybercrime. Businesses trust their advisors with key information to deliver compliance, advisory and credit services, putting significant pressure on firms to keep themselves secure. This also makes accountants a prime target.

Cybersecurity and compliance

The UK Department for Science, Innovation and Technology (DSIT) is paving the way for enhanced national cybersecurity with its forthcoming Cybersecurity Governance Code of Practice. This initiative, integral to the UK's £2.6 billion National Cybersecurity Strategy, aims to empower directors and business leaders to craft robust cyber governance frameworks, thereby boosting cyber resilience across various sectors.

The Code outlines five core principles: risk management, cyber strategy, people, incident planning and response, and assurance and oversight.

These guidelines are designed to be actionable, offering organisations a structured approach to enhancing their cybersecurity postures. Given the degree to which SMEs rely on their advisors for compliance, accountants will need to take a leading role in making their businesses and clients secure.



What are the threats facing businesses?

1. **Phishing:** The UK is the biggest target for phishing attacks in Europe, affecting 96% of businesses. Phishing involves cybercriminals impersonating trusted sources to deceive recipients into clicking malicious links or divulging sensitive information. These attacks can be sophisticated, mimicking legitimate communications to a tee, and can occur across various digital platforms, including email and messaging services.
2. **Data Breaches:** 2023 saw a 17% increase in data security incidents in the UK. These incidents involve unauthorised access to, or acquisition of, sensitive, protected, or confidential data. Data breaches can be external or internal, with the latter sometimes resulting from innocent errors by employees. Regardless of the source, the impact can be devastating, leading to significant financial and reputational damage.
3. **Ransomware:** A growing threat, ransomware attacks reached record levels last year, with criminals compromising data on potentially more than 5.3 million people from over 700 organisations. In a ransomware attack, cybercriminals infiltrate and lock access to key files or systems, demanding a ransom to restore access. These attacks can cripple operations, preventing access to crucial information and systems until the demanded payment is made or the issue is resolved through other means.
4. **Malware:** A broad category that includes various forms of malicious software designed to infiltrate, damage, or disable computers and computer systems. Malware can steal, encrypt, or delete data, alter or hijack core computing functions, and spy on users' computer activity without their knowledge or consent.

How does AI affect cybersecurity?

The launch of consumer facing tools like ChatGPT has fired the starting pistol on a race to implement AI tools in businesses, but it's incumbent on accountants to ensure that these tools are used responsibly within and outside their practices.

While AI can theoretically boost defences by identifying unusual patterns and predicting potential breaches, AI systems themselves can be targets of sophisticated cyberattacks. For firms using AI tools to process client data, this involves understanding its limitations, ensuring transparent data handling processes, and maintaining up-to-date security protocols to mitigate risks.

How can accountants protect their businesses and clients?

Maintaining client trust and security requires a proactive approach to security at all stages of your workflows. The majority of cybersecurity measures are intuitive and common sense – the key is diligent implementation and review within your practice and training.

1. Managing passwords

Strong, unique passwords are the cornerstone of good cybersecurity hygiene. Using the same password across multiple accounts significantly increases the risk of a security breach.

- Encourage regular password updates and educate your team on the importance of password complexity.
- Implementing two-factor authentication (2FA) adds an essential layer of security, combining something you know (your password) with something you have (a code sent to your device), significantly reducing the likelihood of unauthorised access.

2. Controlling access and profiles

Modern software enables you to define access levels within your firm and control the flow of information between stakeholders.

- Tailor user access based on individual role requirements, minimising unnecessary exposure to sensitive information.
- Monitor sign-in activities, especially from unusual locations or devices, to detect potential security threats promptly.
- Avoid using public Wi-Fi for work-related tasks; if necessary, utilise a VPN to secure your connection.

3. Safeguarding your software

As threats evolve, it's essential to ensure your tools keep up. Software providers should offer regular updates to keep their platforms secure, but this only works if you remember to engage with them.

- Keep all software, including operating systems and applications, up-to-date to protect against known vulnerabilities.
- These often include patches for security loopholes that could be exploited by cybercriminals.
- Ensure that your network is safeguarded by a reliable firewall, which serves as a barrier between your internal network and external threats.
- Maintain updated anti-virus software to defend against malware, spyware, and ransomware attacks.

4. Good Data Hygiene

The more data you hold, the more you're at risk of a breach. That's why the easiest way to keep information safe is to store as little as possible.

- Adopt a data minimisation approach – collect and store only the data that is essential for your practice and client servicing.
- Comply with GDPR by systematically deleting outdated or unnecessary information, reducing the risk of both compliance violations and data theft.
- Utilise encrypted communication to safeguard data at rest and in transit, making it unreadable to unauthorised individuals.

5. Team training

Your people can be your biggest asset, or your biggest risk when it comes to security. That's why education is as important as tools for staying safe.

- Regular training sessions can help keep your team informed about the latest threats and best practices.
- Keep conversations open – it's far better to be honest about a mistake and learn from it rather than keep it hidden and let it spread.
- Encourage a culture of awareness, where employees are proactive in identifying suspicious activities and knowledgeable about the procedures to follow in case of a potential breach.

6. Cyber insurance

Cyber insurance offers accounting firms a critical layer of financial protection against cyber threats, complementing their cybersecurity defences. It covers expenses related to data breaches, network damages, and legal costs, reinforcing the firm's resilience against cyber incidents.

- By securing a policy, accountants can assure clients of their commitment to data security, potentially mitigating reputational risks associated with cyberattacks.
- Tailored policies allow firms to address specific vulnerabilities, providing financial stability and support for incident response and recovery processes.

Creating your cybersecurity plan

Keeping your firm safe doesn't require you to become a cybersecurity expert overnight, but it does require planning and attention.

1. **Evaluate the risks:** Catalogue all sensitive data, including client and financial records in your businesses, as well as the risks associated with all hardware and software, pinpointing vulnerabilities.
2. **Set your policy:** Set standards for data protection, password protocols, and device usage. including guidelines for remote work, incident response, and reporting security breaches.
3. **Segment users and teams:** Restrict data access through role-based permissions, ensuring users access only what's necessary for their roles, along with strong, unique passwords and multi-factor authentication for enhanced security.
4. **Secure your environment:** Utilise firewalls, intrusion detection systems, and encryption to protect your network and update all software and firmware to address security vulnerabilities.
5. **Backup and Recovery:** Establish a routine for data backup and verify the effectiveness of your recovery plan.
6. **Perform Regular Audits and Assessments:** Schedule periodic reviews of your cybersecurity measures to identify and address potential weaknesses.

How to choose the right software for your business: A checklist

Your choice of accounting software is the front-line defence for your clients financial data. When comparing solutions, ensure that you consider:

- **Security features:** Ensure the software comes equipped with robust security infrastructure, including encryption, firewalls, and intrusion detection systems.
- **Compliance with industry standards:** Check that software adheres to relevant industry standards and regulations, particularly those concerning data protection and privacy.
- **Access control:** Look for detailed user access controls, allowing you to define who can view, edit, or share your business information.
- **Regular updates and support:** Choose a provider that offers consistent updates and support to address emerging security vulnerabilities.
- **Disaster protection:** Ensure that the software includes reliable backup and recovery solutions to prevent data loss in case of a cybersecurity incident or system failure.
- **Integration capabilities:** Assess whether the software can securely integrate with your existing systems and tools, minimising risk from data in transit.

Bright's suite of accounting tools include industry-leading multi-layered security and compliance with stringent certifications like ISO 27001 & Cyber Essentials. With specialised measures like regular security training, phishing defences, multi-factor authentication, and advanced device and network protections, Bright ensures the safeguarding of your clients' data at every stage to ensure complete peace of mind.

About Bright

Founded in 2021, Bright is a leading provider of accounting, payroll, tax, and practice management software. We're on a mission to make a happy and efficient working life a reality for accountants through reliable software and amazing support.

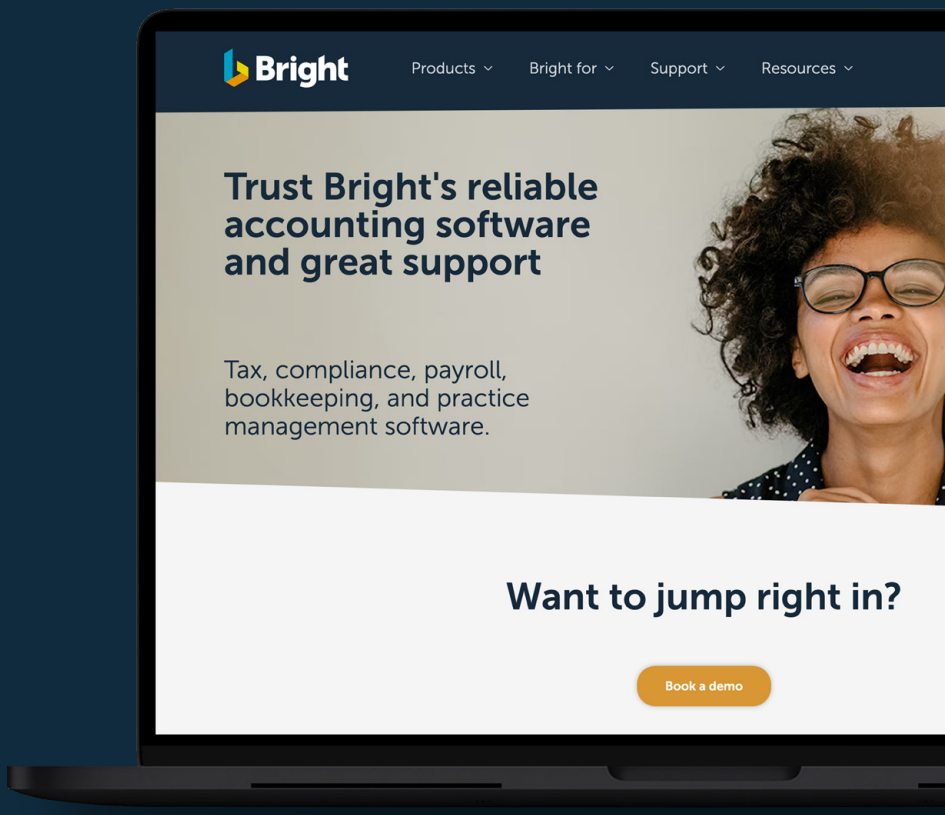
Interested in learning more about how we help accountants like you?

Book a demo

400,000
Businesses using Bright products

98%
Bright customer satisfaction rate

30+
Years' industry experience



Bright

Simply brilliant software

www.brightsg.com