

The invisible threat: Identifying and mitigating cyber risks in accountancy



Welcome to today's webinar



CPD
CERTIFIED
The CPD Certification
Service

 Bright

Agenda

1. What is cybersecurity?
2. Cybersecurity statistics
3. 5 common cybersecurity threats to accountants
4. The consequences of a data breach
5. Cybersecurity best practices for you and your clients
6. How cloud-based technology can enhance cybersecurity
7. How does AI affect cybersecurity?

 Bright



What is cybersecurity?

- A digital guard that protects devices connected to the Internet from unauthorised users
- Cybersecurity includes a combination of software tools, as well as smart online habits

UK cybersecurity statistics



32% of businesses recalled a cybersecurity breach in the previous 12 months



Only 3/10 businesses have undertaken cyber security risk assessments in the last year



Approx 2.39 million instances of cyber-crime in the previous 12 months



Only 68% of microbusinesses say cybersecurity is a high priority



Breaches cost each business, of any size, an average of approximately £1,100



How are accountancy practices at risk?

- Firms are at high risk of cybersecurity attacks due to the valuable information they handle
- Accountants frequently transfer large volumes of data between their firm, clients, banks, and regulatory bodies



5 common cybersecurity threats

1. Phishing attacks



An attacker deceives an individual into sharing sensitive information by posing as a trusted entity



May be conducted by email, SMS, social media and other methods



2. Malware attacks



Harmful software gets onto someone's computer aiming to damage or steal information



82% of ransomware attacks in 2021 were against companies with fewer than 1,000 employees



3. Remote working cybersecurity threats



With employees working remotely from various locations, cybersecurity risks increase



The use of public Wi-Fi can lead to data being compromised



4. Human error



Happens when someone accidentally exposes sensitive information



Almost 88% of data breaches are due to human error



5. Insider threat



Someone misuses their access to expose sensitive information



An organisation's security can be put at risk



Consequences of a data breach



Loss of client trust



Increased insurance premiums



Regulatory fines & sanctions



Reputation damage



Legal actions

Consequences of a data breach



Operational disruptions



Cost of remediation



Impact on talent retention & acquisition



Long-term financial impact

Cybersecurity best practices for accountants

- > Regular security audits
- > Employee training and awareness
- > Use strong password policies
- > Implement access controls
- > Secure email communications
- > Regular software updates



Cybersecurity best practices for accountants

- Incident response plan
- Backup data regularly
- Cybersecurity insurance
- Client data protection policies
- Regularly review third-party providers
- Evaluate software from a security perspective



Remote working security

- Establish clear remote working policies
- Secure Wi-Fi networks
- VPN for remote access
- Employ endpoint protection



Cyber security best practices for clients

- Client education and awareness
- Leverage technology solutions
- Regular communication
- Implement secure collaboration tools



Leading client adoption of secure practices



Educate on the importance



Simplify the transition



Offer training & resources



Be patient & accessible

Upcoming webinar:

Balancing books and well-being: How the software you chose can help create a better work-life balance

Tuesday, 4th June, 11:00 am



How using cloud-based technology can help keep your data safe



Enhanced security measures



- > Cloud service providers typically invest heavily in security technologies

Automated backups



- > Cloud-based applications often include automated data backup features

Access control



- Cloud applications usually allow for granular access controls

Data encryption



- Data stored in the cloud is usually encrypted, both at rest and in transit

Regular software updates



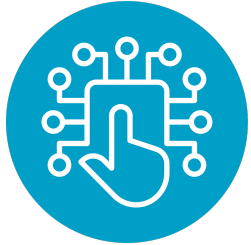
- Cloud software typically updates automatically to the latest version

Disaster recovery capabilities



- Many cloud services offer robust disaster recovery options

Compliance assurance



- > Cloud providers often comply with various industry and governmental data protection standards

Secure data transfer methods



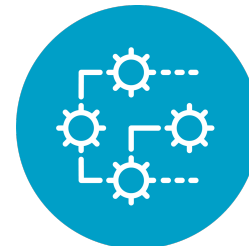
- > It's paramount for accounting practices and their clients to adopt secure methods for transferring sensitive information

Digital record keeping



- > Encouraging or mandating digital record-keeping can significantly enhance security and efficiency

Integrations



- > When accounting tools are integrated, data can be transferred seamlessly between systems



Home to award-winning payroll, accounting, practice management, tax and HR software

 **Bright Pay**

 **Bright Manager**

 **BrightCoSec**

 **Bright Tax**

 **Bright AccountsProduction**



How does AI affect cybersecurity?

- Artificial Intelligence (AI) stands out as a double-edged sword for accountancy practices
- Navigating this relatively uncharted territory presents both opportunities and uncertainties

Key takeaways

