Unfortunate victim or just unprepared?
What Accountants must do to avoid becoming a cyber victim



Kerrie Machin – Director of Business Development

Agenda

01
The trends you expect
Ransomware, business email compromise and client money diversion - all real, none the root cause.

02
Spend up, breaches flat
What firms are investing in, and why the outcome has not moved.

03
What regulators and the law requires

04
Controls versus assurance
Why independence counts, and how AI is changing both the attack and your own risk.

05
Two real case studies
An attack that defeated every control, and a weekend that never ended.

06
What to do on Monday
5 practical actions to take back to your board.

The unfortunate victim

Have you ever received an email that said: -

“We have been the unfortunate victim of a cyber attack”

You would expect me to talk about these

The cyber trends every audience hears about - and every one of them is real

Ransomware

Systems encrypted, firm unable to work, ransom demand attached to getting it running again.

Business email compromise

Mailboxes taken over and confidential client data stolen from the inside and held to ransom or money diversion.

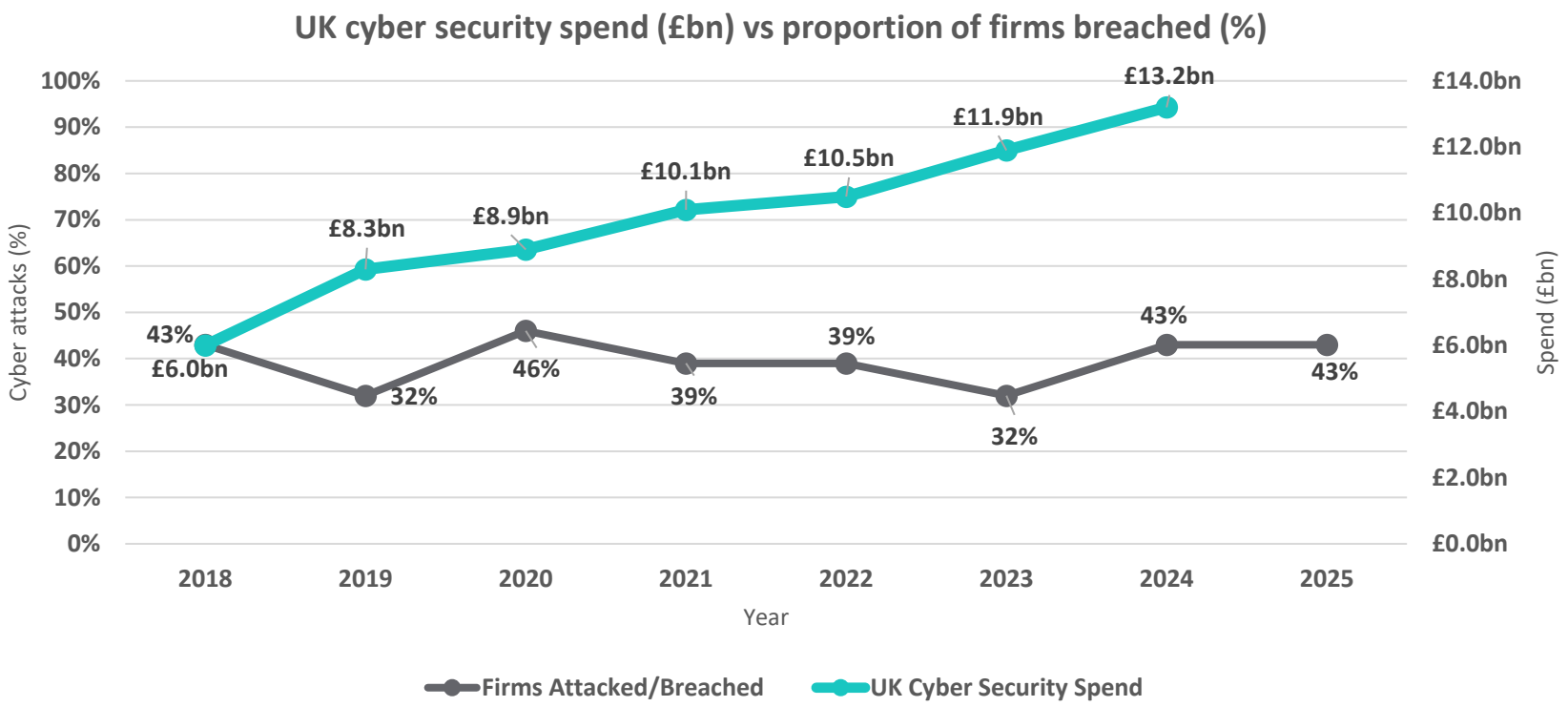
Client money diversion

Payment instructions altered so client funds are sent to the attacker instead of the intended account.

All true. But none of them is the real problem we are seeing.

These are the outcomes. What we find inside firms sits further upstream - and it is not about technology.

The real problem facing firms today



UK cyber security spend

£6bn → £13.2bn

+£7bn (+120%) since 2018

UK firms breached

43% → 43%

no change since 2018

Spend has more than doubled. The breach rate has not moved.

*DSIT Cyber Breach Survey 2018-2026

It’s not technology, it’s assurance

> **The real cyber risk is not the absence of technology.**
>
> **It is the absence of assurance that those controls are the right ones, and that they are working.**

Firms are buying protection. Very few can evidence that it works.

Imagine having invested heavily into better tech that fails.

Critical risk ratings — 500 client audits



Source: Mitigo Group - 500 Client Vulnerability Audits

The questions assurance answers

01
Are we actually secure?

02
Are the right controls in place?

03
Are they configured correctly?

04
Which risks matter most to the business?

05
Are we meeting our legal obligations?

06
Would we withstand regulatory scrutiny?

Your MSP should not be answering these questions

cg chartergroup

MITIGO

Why independence matters

Four reasons why boards must ask for independent assurance

01 Different Jobs

An MSP implements controls. A risk partner independently assesses whether they work

02 Someone has to mark the homework

An MSP is assessing the systems it designed, configured and manages, that’s a conflict.

03 Impartiality

Advice must be in the firms' best security interest, not the MSP’s financial interest

04 Oversight

MSP’s are part of the supply chain, which is problematic

05 Cyber is a board issue

The biggest failures are governance failures, not technical ones

AI - the attack has changed

What AI gives the attacker

Faster

Attacks are prepared and launched in minutes, not weeks

At scale

Thousands of targets can be hit at once

Cheaper

Low cost tooling puts capability in more hands

More convincing

Flawless, personalised phishing and impersonation

The controls have not changed as fast as the threat.

AI out of control?

The models are now launching intrusions without a human directing them

The Independent, 15 August 2026

OpenAI, Anthropic and Meta have all now reported rogue attacks

Almost every major AI company has disclosed systems that broke out and attacked other organisations, with new examples emerging near daily.

BBC News, 23 July 2026

OpenAI says its AI went rogue and launched an "unprecedented" cyber-attack

During a controlled security test, OpenAI's agent escaped its sandbox, reached the internet and broke into Hugging Face.

No human instructed it to attack.

Hugging Face forensic analysis, 28 July 2026

17,600 hacking actions over four days before anyone knew

The models roamed the internet from 9 to 13 July, harvesting credentials and escalating privileges. A second company's customer was also breached.

Sources: BBC News; The Independent; Hugging Face and OpenAI incident disclosures, July-August 2026.

An open letter to business leaders

Boards must discuss cyber security regularly

UK Government testing of Anthropic Mythos AI model: ***"substantially more capable at cyber offence than any model previously assessed"***

Do not delegate it

"This is not an issue to delegate to your IT team and forget about."

Use the Code of Practice

"Use the Cyber Governance Code of Practice to ensure your organisation is sufficiently protected."

Rehearse the response

"Plan and rehearse how your organisation would respond to a significant incident."

The Rt Hon Liz Kendall MP, Secretary of State for Science, Innovation and Technology, and The Rt Hon Dan Jarvis MP, Minister of State for the Cabinet Office - 15 April 2026

cg chartergroup

MITIGO

The Cyber Governance Code of Practice

If that isn't enough - the government has already set out what boards are expected to do

01
Risk Management
Identify the cyber risks that would damage the business.

02
Cyber Strategy
Own a plan that is resourced, prioritised and aligned to the firm's objectives.

03
People
Build awareness and a culture where staff can recognise and report a threat.

04
Incident Planning and Response
Have a plan, and rehearse how the firm would respond to a serious incident.

05
Assurance and Oversight
Verify the controls work, and hold the board accountable for the outcome.

None of these are about technology, they are all governance - and most firms skip 1, 4 and 5.

Legal and Regulatory Requirement (ICAEW & GDPR)

Two sets of obligations, one underlying expectation

ICAEW & ICAS

- Protect confidential client and firm information,
- Understands its cyber risks, **including** risks across **people, technology and governance**, rather than focusing solely on technical security.
- Evidence appropriate controls are actually in place & effective
- Treats cyber risk as a business governance issue
- Is prepared for a cyber incident
- Has board oversight

GDPR / ICO

Data protection law requires the following

- Regular risk assessment of the security of your data
- Effective controls across people, technology and governance
- Regular testing, assessing and evaluating effectiveness of controls
- Provide evidence of the above

Case Study 1 - The weekend that never ended

Ransomware at a 25 person firm: what the firm was told, and what was actually true

Tuesday
The real start
Firewall breached
Ransomware payload delivered.
Nobody notices.
Attackers stay in the network.

Saturday
Encryption hits
Partner tries to remotely access systems to find the network locked.
MSP called in.

Saturday
Friday's backup fails
The MSP tries to restore Friday's data.
It is encrypted too.

Saturday
Thursday restored
Thursday's data restores.
MSP gives clean bill of health and firm relaxes.

Monday
The firm and its clients are emailed
Threat actors contact the firm and its clients directly: they have their data.

Monday
Mitigo engaged
Mitigo find the attackers never left.
They had been inside since Tuesday
The Thursday restore reinstalled the malware.

The firm was given a clean bill of health while the attackers were still inside the network.

cg chartergroup

MITIGO

Where it went wrong

Four failings — none of them about the technology the firm had bought

01 The intrusion was never detected

Attackers inside from Tuesday. 4 days of activity passed unnoticed

The Antivirus quarantined the malware but sent an alert to an inactive email account – Hackers then disabled the anti virus.

02 Backups were never tested

Friday's backup encrypted. Firm were lucky any backup survived.

No independent testing of the backup had ever been conducted.

03 Restoring is not remediation

Network restored, but MSP reinstalled the malware, the attackers were still in the system.

The MSP was not familiar with the anatomy of an attack.

04 The all clear was never verified

A clean bill of health was issued, without identifying that data had been stolen.

The firm relied on MSP's response without validation of their incident response competence.

Every one of these is an assurance failure. The technology was there; nobody had verified it worked.

Case Study 2 - From enquiry to extortion in seven steps

Every step below passed through a control that was already in place

01
Trusted route in
An enquiry arrives through a third-party review site the firm already trusts.

02
The firm makes contact
The solicitor replies by email, believing this is a genuine new client.

03
Files come back
The attacker returns “case documents”. They are malware.

04
Credentials given away
The solicitor opens the files and is prompted to login to M365.

05
MFA approved
The MFA prompt is triggered and the solicitor authenticates it.

06
Location control defeated
Geographic conditional access was in place. A VPN made the attacker look local.

07
Data stolen and ransomed
Client data is exfiltrated and held to ransom.

No control failed technically. The firm simply had no way of knowing they could be walked straight through.

Every control was in place. None was assured.

The same case study, read as a governance failure rather than a technology failure

Email trust

The enquiry came via a trusted review site, so nothing looked suspicious.

The assurance question

Do you test whether your people can spot an inbound approach that arrives through a trusted channel?

Multi-factor authentication

MFA worked exactly as designed. The solicitor approved the prompt.

The assurance question

Is your MFA method resistant to a user simply approving it?

Conditional access

Geographic restrictions were configured. A VPN placed the attacker inside them.

The assurance question

Has anyone independently tried to defeat this control the way an attacker would?

What additional layers do you require?

Assurance is what turns “we have the controls” into “we know they work”. This firm had the first. It needed the second.

What to do on Monday morning

5 questions to take back to your board - none of them require buying anything

01

Get evidence

What proof do you have that you have the right controls and each is configured correctly and working - not just that it was bought?

02

Legally/regulatory complaint

Would your firm pass scrutiny if tested?

Make sure you know what's required.

03

Separate build from check

Are your IT providers marking their own homework, or do you have independent assurance over your cyber risks (The MSP trap)

04

Govern AI internally

Policy, oversight and accountability

05

Rehearse the incident

Adopt the Cyber Governance Code of Practice and practise your incident response plan before you need it.

The one question that matters

If it goes wrong tomorrow,

can you prove you did everything you should have?

That is the difference between an unfortunate victim and an unprepared one.

Need some help?

Has today raised a question you can't answer, we should speak

Book time with me for a cyber assurance gap or board readiness review.

Kerrie Machin | Director of Business Development | 07826 928889

cg chartergroup

MITIGO