



Cyber Security and Financial Governance in Academy Trusts

Taylor Rogers | Partner | UHY Williamson Croft

Liverpool Hope University • Thursday 8 October 2026



About the speaker

Taylor Rogers, FCCA — Partner, UHY Williamson & Croft

Background

- A graduate of Manchester Metropolitan University, Taylor joined Williamson & Croft as part of the firm's 2017 intake and is now a Partner at the firm.

Role

- A familiar face to many of the firm's new clients, supporting them with accountancy and tax needs. He also runs the firm's Professional Partners Network.

Reputation

- Known within the firm as a natural relationship-builder - quick to understand the practical challenges clients face and to build strong working relationships around them.



FCCA

Fellow Chartered Certified
Accountant



Protecting pupils, staff and school finances

Cyber resilience is a whole-school responsibility, not just an IT one.

Helping you prosper



Session overview

1. Part 1: The scale of the risk: real cases and current data
2. Part 2: What's changing under the Academy Trust Handbook 2026
3. Part 3: Practical steps, governance and the questions your board should ask

Why this is a finance issue, not just an IT one

Cyber incidents increasingly manifest as financial losses before they're recognised as security failures - payment diversion, invoice fraud, and business email compromise.

The pattern

- **Attackers don't need to breach a network when they can simply intercept an email and redirect a payment. These frauds succeed by exploiting a gap in internal process, not a gap in technology.**

Framing

- **Robust financial controls are now a core part of cyber resilience - not a separate workstream from your IT team.**

Case study: Wembley Multi-Academy Trust (WMAT)

A real, reported example of payment diversion fraud against a trust running three schools in northwest London.

What happened

- Over the 2022–23 financial year, WMAT made four payments totalling £385,532 to a supplier for construction work. The supplier's email was tampered with, and the payments were redirected to an incorrect bank account.

The aftermath

- The Metropolitan Police launched an investigation. WMAT's own accounts later recorded a further £31,125 in interest charges on a late payment of supplier invoices linked to the fraud - a cost beyond the initial loss.

The lesson

- School business expert Micon Metcalfe:

“Anybody can be susceptible to this type of fraud... [the only way to avoid it is] to be very vigilant around your controls for changing bank account details.”

(Schools Week, Nov 2024)

£385,532

lost to payment-diversion fraud,
2022–23

How this could have been stopped

Not an education-specific fix...the same sequence applies to any organisation that pays suppliers by bank transfer, in any sector.

Step 1: Treat the request as unverified

- A request to change bank details is unconfirmed until proven otherwise - even if it looks entirely legitimate.

Step 2: Call back on a number you already hold, and have used previously

- Never one from the email or invoice. Described by UK Finance and Action Fraud as the single most reliable defence against this type of fraud.

Step 3: Require a second, independent approver

- No one person should be able to both amend a supplier's details and approve payment to them.

Step 4: Test first, then reconcile promptly

- Send a small payment and confirm receipt by phone (refer to Step 2 above) before releasing the full amount – then reconcile within days, not at year-end.

Call first!

verify any bank-detail change by phone, using a number already on file
- never one from the email

The financial anatomy of a cyber incident

Using real-world examples from the education sector - a breach is rarely one bill.

Direct costs

- Business interruption, recovery and forensic investigation, and legal or regulatory costs — Active Learning Trust's 2024 ransomware attack cost over £500,000 and 1,200 staff hours to resolve.

Financial control costs

- Fraud arising from payment diversion and invoice scams — Wembley MAT's £385,532 loss also generated £31,125 in knock-on interest charges the following year.

Insurance and reputation

- Insurance implications (cover, excess and claim complexity) and reputational damage that can affect pupil recruitment and stakeholder confidence.

Key message

- Cyber incidents are often finance crises before they're IT crises.

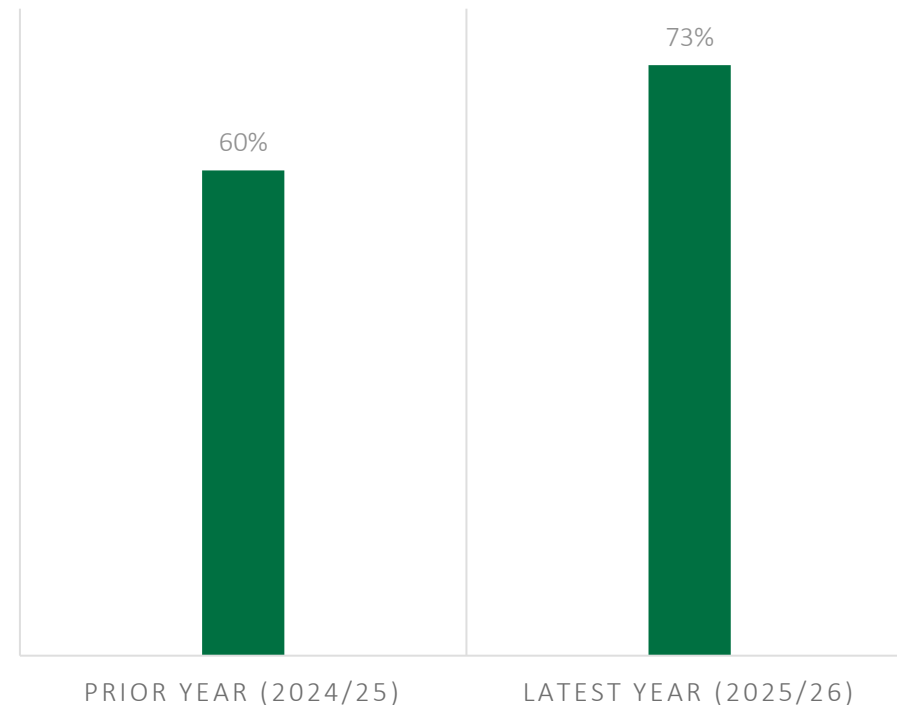
The scale of the threat

73% of secondary schools identified a cyber breach or attack in 2025/26 - up from 60% the year before*.

This is a live and growing risk - every finance team in this room should assume they are a target, regardless of trust size or profile.

***Source: DSIT/DfE Cyber Security Breaches Survey 2025/26.**

SECONDARY SCHOOLS IDENTIFYING A CYBER BREACH



The scale of the threat across education

The same DSIT/DfE survey breaks results down by institution type — the pattern holds across the whole sector. In 2025/26:

Primary schools

- 49% identified a breach or attack - up from 44% the year before.

Secondary schools

- 73% identified a breach or attack - up from 60% the year before.

Further education colleges

- 88% identified a breach or attack - the highest rate outside higher education.

Higher education institutions

- 98% identified a breach or attack - effectively universal exposure.

What's changing under the Academy Trust Handbook 2026

1. Prohibition of ransomware payment or other extortion demands continues - in force since ATH 2025, carried forward unchanged.
2. CFO qualification requirements phase in for trusts over 3,000 pupils.
3. New funding distribution statement required alongside audited accounts.
4. Increased board-level scrutiny of going concern and financial risk.
5. Statutory trust-level Ofsted inspections become law, effective from 2027/28.

The ransomware payment prohibition

Trusts have been legally unable to pay ransomware demands since ATH 2025 (September 2025); ATH 2026 carries this forward unchanged.

Why it matters

- The ban doesn't reduce the risk of an attack — it removes one (bad) option for responding to it. Prevention, backups and recovery planning now carry the full weight of the response.

Part of a wider framework

- The payment ban sits alongside six DfE Digital and Technology Standards trusts are expected to work towards by 2030, covering connectivity, cyber security, and digital governance more broadly.

Case study: Active Learning Trust

- 21 schools across Cambridge and Suffolk, serving almost 9,000 pupils, were hit by ransomware in July 2024. Files were encrypted across 10 sites; the trust had to rebuild its entire server infrastructure from scratch.

The cost

- Over £500,000 and 1,200 hours of staff time - published by DfE as a case study on its own Cyber Security Hub.

£500k+

cost to resolve the July 2024 attack

1,200

staff hours spent on recovery

CFO qualification requirements

A phased-in requirement for trusts over 3,000 pupils — two dates matter.

From 1 October 2026

- Recruitment exercises for CFO roles should specify a qualified accountant — three days after this event.

From 1 September 2027

- This becomes a hard requirement, not just guidance.

Why it's being tightened

- Financial oversight is now a named governance requirement — not an assumption. If you're recruiting a CFO in the next year, plan for this now.

1 Oct 2026

adverts should specify a qualified accountant

1 Sep 2027

becomes a hard requirement

Funding transparency and going concern scrutiny

Three related changes that increase the visibility of a trust's financial position.

New funding distribution statement

- Multi-academy trusts must publish a summary statement by 31 January, alongside audited accounts, showing how funding is distributed across their schools.

A formal duty to flag risk – not just to report it

- Accounting officers must now formally notify trustees where a trust's ability to operate as a going concern may be at risk - moving going concern from an annual accounts exercise into ongoing, active governance.

Reserves and forecasting become standing duties

- Boards are expected to actively manage reserves and support accurate three-year financial forecasting, rather than focusing only on the annual budget.

31 Jan

funding distribution statement due

Statutory trust-level Ofsted inspections

A significant governance change that's now law, though its practical impact is still a year or two away.

What changed

- An amendment to the Children's Wellbeing and Schools Bill, tabled January 2026, received Royal Assent in April 2026.

What it introduces

- Statutory trust-level inspections Statutory trust-level inspections assessing five things: quality of education across the trust's academies, governance and executive leadership, action to promote pupil wellbeing, action to drive school improvement, and the trust's management of its resources - not just individual schools.

Why the 'resources' element matters from a financial viewpoint

- This draws on the existing regularity, propriety and value-for-money framework trustees and accounting officers already assure to the DfE and Parliament every year, but which has never before been subject to independent, public inspection. Weak financial governance - poor segregation of duties, an unmanaged going-concern risk, undocumented spending - currently surfaces through a private DfE financial management review. Once trust inspections begin, the same weaknesses could show up in a public Ofsted judgement instead.

Timing

- Inspections themselves aren't expected to start until the 2027/28 academic year — worth flagging to boards now so it isn't a surprise later.

2027/28

first academic year of trust
inspections

What's changed in internal scrutiny and audit

The scope of internal scrutiny has broadened significantly under ATH 2026 – no longer just about financial controls

Broader assurance scope

- Internal scrutiny must now provide assurance over financial controls, non-financial controls, risk management arrangements, and wider organisational risk - not just payment processes.

Risk based, not checklist-based

- Programmes should be built using a risk-based approach and linked directly to the trust's risk register, rather than working through a generic annual checklist..

A new duty for Audit & Risk Committees

- Committees must ensure that any information submitted to the DfE which affects funding is accurate and compliant — a specific, named assurance responsibility.



Risk-based, not checklist-based /
linked directly to the trust's risk
register

Executive pay, pensions and benefits

Tighter DfE controls on executive remuneration sit alongside one welcome relaxation

Pay can't outpace teacher pay

- Executive pay must not increase faster than teacher pay unless DfE approval is obtained.

New approval thresholds

- DfE approval is required before advertising any role with remuneration above £174,000, or performance-related pay above £25,000.

Pension alternatives now need sign off

- Prior DfE approval is required before proposing any alternative to the Teachers' Pension Scheme (TPS) or Local Government Pension Scheme (LGPS)

One relaxation

Electric vehicle salary sacrifice schemes no longer need prior DfE approval, provided appropriate safeguards are in place.

The reporting threshold and building an anti-fraud culture

Knowing the threshold matters as much as knowing the controls.

DfE reporting threshold: £5,000

- Fraud, theft or irregularity above this level — individually or cumulatively across a financial year — must be reported. Fraud judged “unusual or systematic” must be reported regardless of value.

Building an anti-fraud culture

- Clear fraud policy and response plan, good technical controls, phishing simulations, and staff cyber-awareness training — the human layer matters as much as the technical one.

£5,000

DfE fraud/theft reporting threshold

Practical steps for boards and finance teams

1. Verify every bank detail change

- Documented, non-negotiable process for verifying any change to supplier bank details — an independent callback, not a reply to the same email.

2. Own the risk jointly

- Clear ownership of financial risk at executive level, working jointly with IT/cyber leads rather than in silos.

Practical steps for boards and finance teams (2 of 2)

The remaining two actions, plus two things worth knowing.

3. Reconcile regularly

- Regular reconciliation and monitoring — not reliance solely on year-end reporting.

4. Test the controls...and test them broadly

- Internal scrutiny now covers non-financial controls and wider organisational risk, not just payment verification, and should be built around the trust's own risk register rather than a fixed annual checklist.

Good to know

- FSCS protection is now £120,000 per registered bank (Dec 2025). Internal scrutiny summary reports are due to DfE by 31 December; the £50m revenue threshold triggering a mandatory audit & risk committee is based on last year's audited accounts, not projections..

£120,000

FSCS protection per registered bank

Questions every Trust Board should be asking

1. Do we have a documented process for verifying bank detail changes - and is it followed every time?
2. Would we spot payment fraud before it crossed the £5,000 DfE reporting threshold?
3. Are our reserves and insurance sufficient, given ransom payments remain prohibited?
4. Is financial risk owned jointly by finance and IT, or does it sit with one team alone?
5. When did we last test our financial controls against a real fraud scenario - not just a compliance checklist?



Taylor Rogers

Partner

UHY Williamson Croft

t.rogers@uhy-williamsoncroft.com

www.williamsoncroft.co.uk