zellis

LIVE WEBINAR • TUESDAY 9 JUNE 2026 • 10:00 BST

HOW TO PROTECT PAYROLL CONTINUITY, *WHATEVER HAPPENS*

A practical 40 minutes on security, compliance and operational resilience for payroll teams.

UNLIMIT WHAT'S NEXT

PAYROLL HAS BECOME A TARGET

zellis

Why this matters now.

OPENING

> *"Pay day used to be the most predictable event in the business calendar. Now it is one of the most exposed."*

Threats are sharper

Ransomware and credential attacks now reach payroll systems directly — not just IT.

Rules are tighter

HMRC penalties, audit scrutiny and ESG reporting all assume payroll is in control.

Margins are thinner

Teams are leaner. One absence, one outage and pay day is in doubt.

WHAT WE'LL COVER IN THE NEXT 40 MINUTES

zellis

40 minutes content, 15 minutes Q&A.

00:00	**The problem**	Three scenarios that nearly broke payroll.
10:00	**Security**	Russ Fray — how attackers reach payroll, and how we block them.
20:00	**Compliance**	Neville Cotton — staying audit-ready in a moving landscape.
30:00	**Operational resilience**	Charlotte Claridge — the human and process backstop.
40:00	**Q&A**	Bring your questions — we'll get to as many as we can.

MEET YOUR SPEAKERS

Three perspectives. One outcome: pay day always lands.

Russ Fray

Chief Information Security Officer, Zellis

Leads security across the Zellis group. Thirty years across enterprise security, threat intelligence and incident response.

Neville Cotton

Director of GRP Risk & Compliance

Owns the compliance and audit posture for Zellis. Deep experience across HMRC, ICO and big-four audit environments.

Charlotte Claridge

Head of Payroll Assistance

Runs the Payroll Assistance Service. Thirteen years inside customer payroll teams, including pay days that nearly didn't happen.

PART ONE

Three scenarios that almost *broke payroll.*

They all happened in the last 18 months. Each one is a pay day nearly lost.

THE PROBLEM, IN THREE REAL STORIES

zellis

Different industries, different attackers, same exposure.

CYBER

UK retailer, credential attack

Attackers used stolen credentials to enter HR systems mid-cycle. Payroll team locked out for 72 hours. Pay day made it — only because the team improvised.

KEY PERSON

The only person who knew

A senior payroll manager was off unexpectedly the week of cut-off. The undocumented bonus calc went with them. Pay was right, but only after a 30-hour scramble.

SUPPLIER

Utilities provider, SaaS outage

A third-party time-and-attendance feed went down for 36 hours. No fallback feed, no manual route. Two thousand variable-pay employees underpaid that month.

WHY PAYROLL IS MORE VULNERABLE THAN EVER

Cyber risk is up. Compliance keeps tightening. And the teams running payroll are smaller than ever.

72%

of organisations say cyber risks have risen in the past 12 months*

£3.58m

average cost of a UK data breach, staffing shortages add a further £1.76m*

1:375

median ratio of payroll professionals to employees in UK in-house teams*

Three shifts behind the numbers

The threat landscape has widened

Payroll holds the richest data, names, bank details, NI, salaries. And the supply chain is longer than ever: T&A feeds, benefits, banking, HMRC integrations. Every connection is an inroad.

The compliance bar keeps rising

Every FPS is a hard deadline, with automatic HMRC penalties for late submission. One missed cycle isn't just operational, it's regulatory.

The team running it is smaller than ever

Most in-house teams run on 1–3 people, processing hundreds of payslips a month. One absence becomes a single point of failure.

**Sources: WEF Global Cybersecurity Outlook 2025 · IBM Cost of a Data Breach 2024 · CIPP & Dayforce, Payroll Insights Report 2025 (in-house).*

HOW PAYROLL FAILS — THREE PATHWAYS

zellis

Most outages we see fall into one of these three buckets.

SECURITY

Someone gets in

Credential theft, ransomware, insider misuse. The system is fine — the access isn't.

Covered next by Russ

COMPLIANCE

The rules shift

A regulation, a deadline, a reporting change. Payroll is right — until it isn't.

Covered next by Neville

OPERATIONAL

A person or process drops

Sickness, supplier outage, undocumented logic. Pay day is in doubt.

Covered next by Charlotte

PART TWO · SECURITY

Russ Fray

Chief Information Security Officer

"You won’t out-build the attackers. You can absolutely out-prepare them."

HOW ATTACKERS REACH PAYROLL

Four routes we see again and again.

01

Stolen credentials

Reused passwords, MFA fatigue, session-token theft. The most common route — and the most preventable.

02

Phishing into HR

HR mailboxes get masses of attachments daily. One opened CV in the wrong place is enough.

03

Third-party compromise

A benefits portal or T&A vendor is breached. The attacker walks in via the integration you trust.

04

Insider error or misuse

Over-broad permissions, shared logins, a leaver who still has access. Rarer, but the highest-impact.

WHAT "SECURE PAYROLL" LOOKS LIKE

zellis

Five controls that move the needle most.

01	**Phishing-resistant MFA on every payroll login**	Passkeys or hardware tokens. SMS isn't MFA in 2026.
02	**Least-privilege access, reviewed quarterly**	No standing admin. No shared logins. Joiners-movers-leavers run on a schedule, not a ticket.
03	**Segmented payroll environment**	A breach in HR shouldn't touch payroll. A breach in payroll shouldn't touch banking.
04	**Tested backups, not "we have backups"**	Restore drill once a quarter — including a full pay run from yesterday's backup.
05	**A run-book the whole team has actually read**	Who calls whom in the first hour. What the manual fallback pay file looks like. Where keys live.

PART THREE · COMPLIANCE

Neville Cotton

Director of GRP Risk & Compliance

"Compliance isn’t a checklist. It’s the evidence trail you can produce on a Monday morning."

WHAT'S CHANGING IN YOUR COMPLIANCE POSTURE

Four shifts payroll teams should already be planning for.

HMRC penalty regime tightening

Real-time information errors and late submissions now carry steeper, faster penalties.

DSAR & GDPR pressure

Employee subject-access requests are rising. Payroll data is at the centre of everyone.

ESG and pay-gap reporting

Public reporting expectations are widening and auditors now expect payroll data to back it up.

Audit trail expectations

Auditors expect not just "what changed" but "who approved it, when, why" — to the field.

AUDIT-READY, EVERY MONDAY MORNING

The compliance routine that holds up under scrutiny.

The weekly compliance loop

- RTI submissions reconciled — every payroll, every week.
- Permissions review on payroll roles — leavers off, joiners scoped.
- Change log signed — every pay-rule change has an owner and a reason.
- DSAR & rights-request queue — nothing older than the SLA.
- Audit evidence folder — current period closed, archived, retrievable.

The one habit that matters most

Capture the reason behind every change at the moment it happens. "Approved by X because of Y" is the evidence auditors and tribunals want — and the one thing nobody can reconstruct six months later.

— Neville

PART FOUR · OPERATIONAL RESILIENCE

Charlotte Claridge

Head of Payroll Assistance

"When systems hold, people are what runs payroll. When systems fail, people are the only thing left."

WHERE PAYROLL TEAMS ACTUALLY BREAK

From 13 years inside customer teams — the patterns that keep showing up.

Knowledge in one head

The senior payroll lead holds the bonus calc, the off-cycle process, the workaround. No back-up.

Locked out mid-cycle

Systems are locked mid-cycle. No access. Pay day is days away. No tested fallback.

Reconciliation skipped

Pay-to-GL or PAYE recs deferred under pressure. Small variances turn into HMRC headaches.

Volume spikes with no slack

Bonus cycle, year-end, mass joiners. The team is full-capacity already.

PAYROLL ASSISTANCE: THE OPERATIONAL BACKSTOP

From 13 years inside customer teams — the patterns that keep showing up.

COVER	CAPACITY	PROJECT	CONTROL
Payroll Continuity	**Pay Assist Support**	**Payroll Project Cover**	**PAYE Reconciliation**
Cover for key-person loss, cyber incident or IT failures. Your team's safety net.	Extra capacity for critical pay cycles, covering absence, attrition and peak demand.	BAU runs while your team focuses on the project, go-live or transformation.	A clean monthly close. We reconcile, you sign off.

WHAT YOU CAN DO THIS QUARTER

Practical steps, no big programme required.

01	**Run a 60-minute payroll continuity stand-up**	Map who does what, who covers whom, where the gaps are. One meeting, real list.
02	**Turn on phishing-resistant MFA on every payroll login**	If anyone still logs into payroll with a password and an SMS code, fix that first.
03	**Document the three things only one person knows**	Bonus calc, off-cycle process, the integration that broke last time. Write them down.
04	**Schedule one restore drill this quarter**	Pick a pay run. Restore from yesterday's backup into a sandbox. Time it.
05	**Take the Payroll Continuity diagnostic**	Eight questions. A scorecard against four resilience pillars. Free, no obligation.

FIVE THINGS TO TAKE BACK TO YOUR TEAM

If you remember nothing else from today.

1. Payroll is a target now, treat it like a finance system, not a back-office tool.
2. Most outages are people-shaped, not tech-shaped. Cover the people first.
3. Audit-readiness is a habit, not a project. The reason-for-change note is the asset.
4. A run-book the team has read beats a perfect run-book nobody has opened.
5. You don’t need a programme to start; you need eight questions and an hour.

OVER TO YOU

Thank you, and a few next steps.

Take the diagnostic

Eight questions. Your scorecard against four resilience pillars.

zellis.com/focus/payroll-assistance-services/

Read the brochure

Payroll Assistance Services, what we do and how we engage.

zellis.com/focus/payroll-assistance-services/

Questions. Drop them into the chat — we'll cover as many as we can in the next 15 minutes of Q&A.