National Lead Force
National Delivery Plan Performance Report

FY 2025/26
Q3: October – December 2025

Performance Assessment

The dashboard provides an assessment of national policing performance against the objectives set out in the **National Policing Strategy for Fraud, Economic and Cyber Crime 2023-28**. The National Policing Strategy was launched in November 2023 and translates national strategies and objectives set by His Majesties Government into actionable measures for policing in the areas of fraud, money laundering and asset recovery and cyber. The report shows national attainment against the objectives. The National Policing Strategy sets out a purpose to "improve the UK policing response to fraud, economic and cyber crime" through three **key cross cutting objectives** of: Improving outcomes for victims; Proactively pursuing offenders; Protecting people and business from the threat

The NLF plan seeks out **key cross cutting enabling commitments** that City of London Police is seeking to achieve		**FYTD Performance**	**Data Trend**
Money Laundering Asset Recovery 1	We will increase disruptions against money laundering offenders.		⇧
Money Laundering Asset Recovery 2	We will seize and restrain more criminal assets through including released asset denial activity		⇧
Money Laundering Asset Recovery 3	We will provide training to policing on how to investigate and seize crypto assets. We will ensure accurate records of crypto assets seizures are maintained and provided.		⇧
Fraud 1	We will increase the policing response and outcomes linked to National Fraud Intelligence Bureau/ Fraud and Cyber Crime Reporting Analysis System crime dissemination packages.		
Fraud 2	We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The National Fraud Squad teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.		⇧
Fraud 3	We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in National Economic Crime Centre led fraud intensifications throughout the year.		⇧
Fraud 4	We will support and assist the national development and implementation of the Fraud Targeting Cell by contributing resource and supporting the delivery of systems and processes. We will increase intelligence packages into the system leading to increased proactive operations.		⇩
Fraud 5	We will develop and deliver a centrally co-ordinated National Fraud PROTECT Network that will align with the National Cyber PROTECT Network, share best practice, and promote local delivery of national messaging.		⇧

Performance Assessment

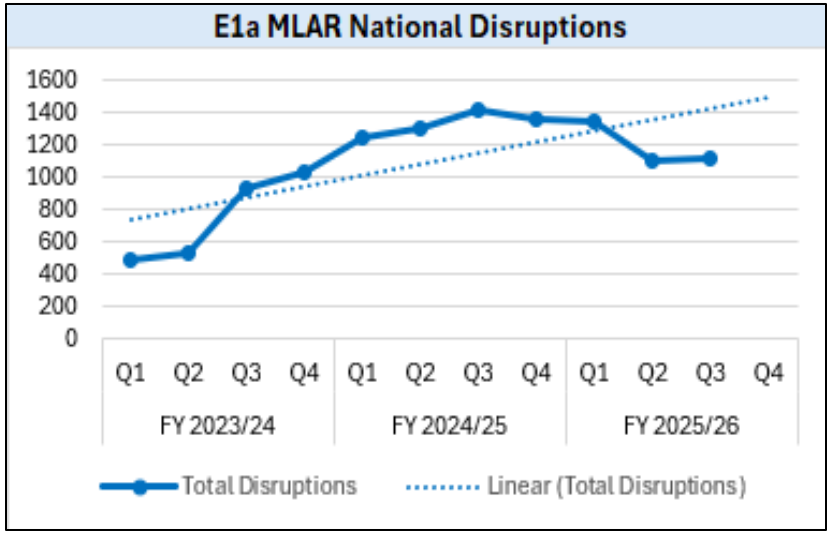
		FYTD Performance	Data Trend
Cyber 1	We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages. We will ensure full and timely compliance from forces to record disseminations from the NFIB appropriately and that subsequent outcomes are reported back to NFIB correctly.		⇧
Cyber 2	We will increase intelligence led proactive operations and self-development operations regarding Computer Misuse Act offending, ensuring the relevant deconfliction safeguards are followed.		⇩
Cyber 3	We will develop the current PROTECT notification processes to ensure a consistent approach to both the direct PROTECT officer taskings and the notifications delivered at scale.		⇧
Cyber 4	We will ensure ROCUs and Forces are regularly using Police Cyber Alarm to help support member organisations when issues are identified and use the data to inform and drive PROTECT, PREVENT and PURSUE activity. PROTECT Officers will promote Police Cyber Alarm to all SME organisations they engage with.		⇧
Cyber 5	We will deliver the new NPCC Cyber Resilience Centre (CRC) Model. This includes the new Operating Model to deliver the levels of consistency and assurance required. CRCs and PROTECT officers will work together to support each other's work and grow CRC membership.		⇧
Cyber 6	We will develop improved referral process for new nominals to include Target Operating Model and definition of when a referral should be made. We will introduce a single national or regional referral mechanism and implement risk assessment (CORA) and tasking mechanisms for PREVENT referrals.		⇧
Cyber 7	We will roll out the Cyber & Digital Specials & Volunteers (CDSV) Programme and platform to every region and Force and ensure effective management and utilisation of CDSV skills across the network.		⇩
Cyber 8	We will revise and roll out a clear training, CPD and accreditation pathway for all roles within TCUK, with regular reviews of the training needs analysis and advancements in technology / threats. NPCC Deliver new strategy and delivery with the Economic and Cybercrime Academy.		⇩

Money Laundering and Asset Recovery

Improve Outcomes for Victims

Performance Measure 1: We will increase disruptions against money laundering offenders.

Success Measures:	FYTD Performance	Data Trend
E1a Increase the number of recorded disruptions linked to money laundering and or illicit finance – **Home Office Measure**		⇧



Op Machinize 2

Operation Machinize 2, led by the National Crime Agency (NCA) ran throughout October and targeted economic crime on the high street with businesses being used as a cover for a wide range of criminality with a real focus on the laundering of funds from that criminality.

This operation involved 2,734 premises visited, 923 arrests and £538k of cash seizures. So far nationally there have been 226 disruptions under the name Op Machinize for Q3.

Analysis

E1a Money laundering and asset recovery (cash confiscation/cash seizure/recovered assets) is classed as illicit finance on APMIS.

In Q3 (October – December), there were a total of 1,117 disruptions.

- 71 major disruptions - 15% increase (+9) in comparison to Q2 25/26
- 170 moderate disruptions - 4% decrease (-7) in comparison to Q2 25/26
- 876 minor disruptions - 1% increase (+9) in comparison to Q2 25/26.

The top 3 disruption types are asset denial & ancillary orders at 51% (690), seizures at 20% (273) and investigative suspect disruptions at 13% (171).

In comparison to the previous quarter (Q2), MLAR disruptions are reporting a 1% increase (+11). In comparison to the same quarter for the previous year (Q3 24/25), there has been a 21% decrease (-294) in MLAR disruptions.
The benchmark from 24/25 is 5,323, which translates to 1,331 disruptions per quarter. For Q3, disruptions are 10% (-418) below the benchmark target, however, disruptions have increased compared to the previous quarter.

Response

In Q3, operational activity contributed to a rise in disruptions, in particular Op Machinize 2. This was the largest operation of its kind focused on rooting out the economic crime and grey economy that makes our high streets less safe and prosperous.

Issues with properly recording disruptions is still on-going, attributing disruptions to the correct operations and ensuring operation names are added upon entry. This can give better insight into the outcomes of intensifications and operations to allow for best practices to be identified. The work to continue this continues to be a key focus of the NPCC Serious and Organised Crime portfolio and COLP is working with the NCA to support this across policing colleagues where possible.

This is a continuing recording issue and not a direct performance issue relating to MLAR disruptions.

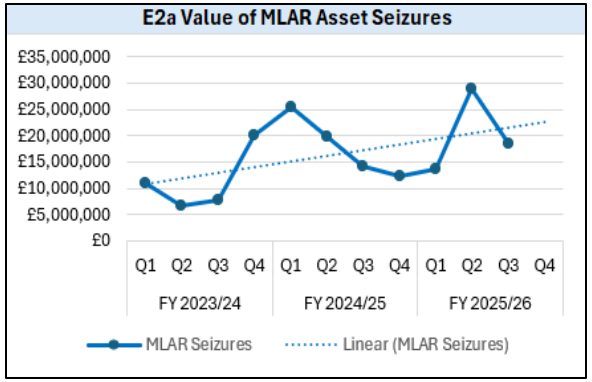
We are expecting to see a rise in disruption activity continue Q4 as planned operations take place and as disruptions are recorded against Op Machinize 2 as investigations progress.

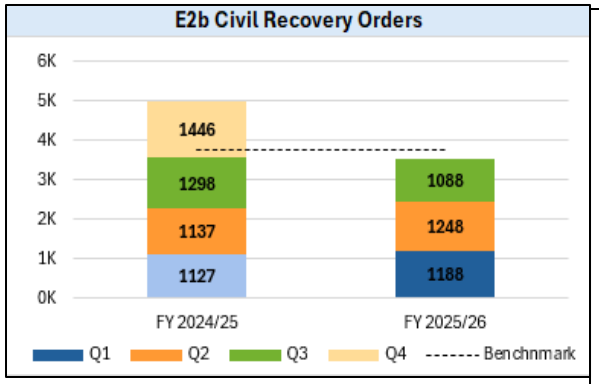
Money Laundering and Asset Recovery

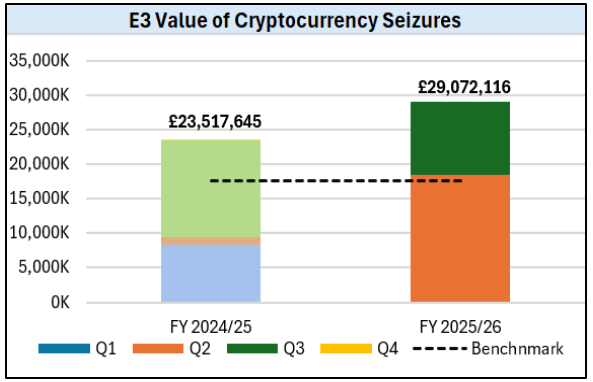
Proactively Pursue Offenders

Performance Measure 2: We will seize and restrain more criminal assets through including released asset denial activity
Performance Measure 3: We will provide training to policing on how to investigate and seize crypto assets. We will ensure accurate records of crypto assets seizures are maintained and provided.

Success Measures:	FYTD Performance	Data Trend
E2a Increase the number of asset freezing orders, restrained assets, and recovered and confiscated assets.		⇧
E2b Increase the number of Civil Recovery Orders.		⇩
E3 Recover a higher number of crypto assets.		⇧







Analysis

E2a In Q3 (October – December), a value of £18,615,212 asset seizures was recorded for money laundering and asset recovery. In comparison to the previous quarter, this is a 36% decrease (-£10,386,302), however Q2 was a highest reporting quarter in the previous three years. In comparison to the same quarter for the previous year (Q3 24/25), this is an 30% increase (+£4,301,737). For 24/25, asset seizures were reporting a downward trend, 25/26 has shown improvement and is 13% above the Q3 benchmark for 24/25 (+£7,177,156). Asset seizures are opportunity-driven, intelligence led and legally constrained which can cause sporadic data trends. Op Machinize 2 reported £2,789,515 in estimated seizure value for Q3, this accounts for 15% of seizures for Q3.

E2b Civil recovery figures in Q3 are reporting a 13% decrease (-160) in comparison to the previous quarter (Q2) and a 16% decrease (-210) in comparison to same period in 24/25 (Q3). Q3 is reporting 6% below the quarterly benchmark for 24/25, although Q3 was a low month, we are maintaining consistent levels of civil recovery orders.

E3 For Q3, there has been £10,611,753 in cryptocurrency seizures, overall, the Q3 benchmark is £17,638,234, Q3 is reporting 65% above the target (+£11,433,882). Although Q3 is reporting a 42% decrease in comparison to Q2, Q2 was a very high month for cryptocurrency seizures and overall, 25/26 is reporting a large increase, surpassing the benchmark for 24/25.

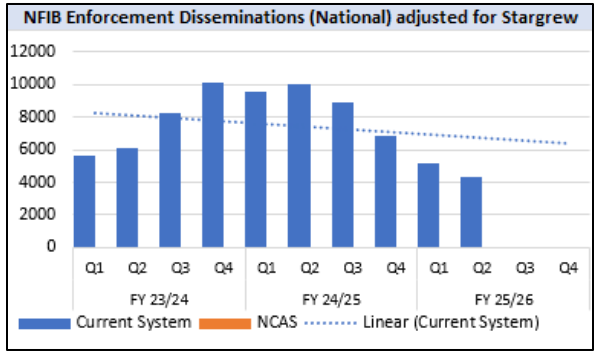
Cryptocurrency seizure figures are currently reported here in the same way as disruption activity via the APMIS tool hosted by the NCA. This is not the ideal reporting method and this causes limitations in what can be reported as well as concerns over accuracy of data reporting. More work is on-going to obtain data from Komainu the national crypto currency vault and the introduction of a new Asset Recovery reporting tool (ARIT) later in 2026 will improve reporting capabilities and performance understanding significantly.

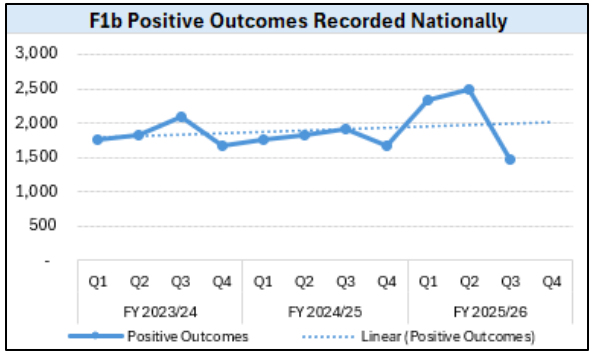
Fraud

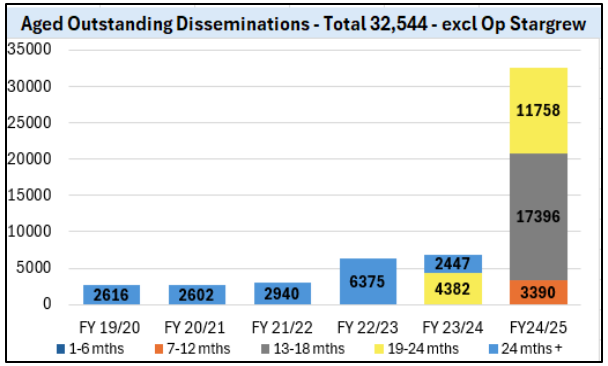
Improve Outcomes for Victims

Performance Measure 1: We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages.

Success Measures:	FYTD Performance	Data Trend
F1a Increase the number of NFIB Pursue disseminations		
F1b Improve the positive outcome rate		
F1c Reduce the percentage of crime disseminations not yet assigned an outcome		⇧







Please note no Q3 data is included in F1a and F1b graphs have been calculated using the legacy systems rather than the new National Crime Analysis System (NCAS) this quarter and will only represent partial outcome volumes, therefore success measure status has not been included. The delivery of Report Fraud Reporting Analysis and Victim Services went live on 4th December 2025 with a public launch on 19th January 2026. The data platforms and reporting processes are still being refined and it has not been possible to provide like for like information to be reported on for this performance product. However some initial data Total number of Pursue Packages Disseminated between Go live on the 31st December 2025 1120 with 1963 crime reports within them. 371 of these were automated Call for service disseminations which previously would have required a manual review and input from the service.

F1b Nationally, there have been 1,478 positive outcomes during this period and 9,177 no further action outcomes. Overall, there is a 13% positive outcome rate. This is a 7% decrease on Q2 24/25, with a positive outcome rate of 20% and a 5% decrease in positive outcomes in comparison to the same period for the previous year (Q3 24/25). The quarterly target of 3,571 has not been met and positive outcomes are reporting 36% below the benchmark for Q3 (-1,270).

F1c In Q3, **32,544** NFIB disseminations from 19/20 to 24/25 had not been matched to an outcome. This is a decrease (which is positive) of 3% (-1,105) from the previous quarter and an increase of 8% (-2,523) from Q3 24/25. As in F1a, Op Stargrew disseminations have been excluded. A large proportion of these are with a single force and engagement attempts continue to try and reduce this. The next stage of this work is to identify a benchmark for what is a normal proportion of disseminations to be in ongoing investigations.

Outcomes

Against the comparative period last year positive outcomes in the legacy system for Q3 were down by 38%, (-889).

This is due to Q3 25/26 not containing any large one-off cases from forces, thus averaging circa 500 per month (i.e. a run rate of circa 6,000 per annum).

For the year to date 9 months to 31st December 2025, total positive outcomes were **6,340**, up **122 (+2%)** on the prior year

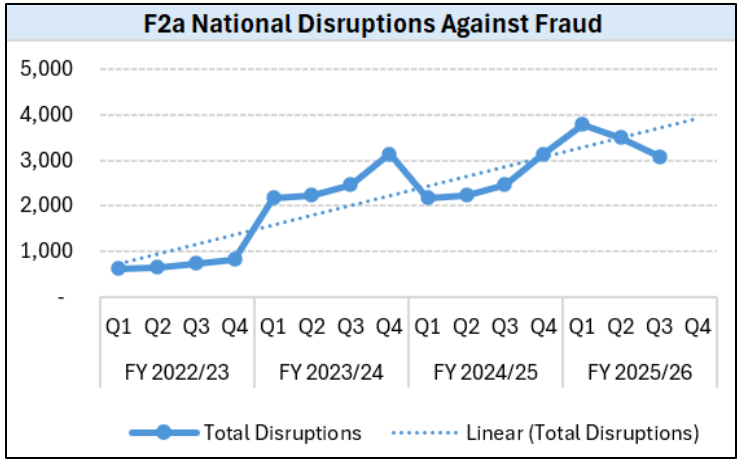
Key drivers across the first 9-month period include an Investment Fraud operation from NLF CoLP yielding 1,199 outcomes in September.

Fraud

Proactively Pursue Offenders

Performance Measure 2: We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The NFS teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.

Success Measures:	FYTD Performance	Data Trend
F2a Increase the number of disruptions against Fraud		⇧



Op Callback 2

Op Callback was an 8-week intensification focusing on Courier Fraud, this operation resulted in 37 disruptions for Q3. (More details on Op Callback 2 in slide 9)

OP ROME - NEROCU

Op Rome involved raising awareness of financial crime amongst business and communities. Messaging was provided direct to employees promoting vigilance around the human element of fraud and common economic attacks. Officers encouraged tactics, behavioural change and understanding of risks. This operation resulted in 119 minor disruptions for Q3, the largest reported disruption recording for this quarter.

F2a Nationally, there were 3,074 disruptions recorded for Q3 (October-December). Q3 was a low reporting month with a 12% (-421) decrease compared to the previous quarter. Q3 is reporting a 25% increase (+607) in comparison to the same period for the previous year and is 38% (+2,846) above the quarterly target, therefore, overall disruption performance is good.

For fraud related disruptions there were:

- 16 major disruptions - 41% decrease (-11) in comparison to Q2 24/25.
- 161 moderate disruptions - 13% increase (+19) in comparison to Q2 24/25.
- 2,897 minor disruptions - 13% decrease (-429) in comparison to Q2 24/25.

Overall, adult safeguarding is the highest disruption type at 36%, followed by specialist advice at 24%. Investigative suspect disruptions also reported high level disruptions at 11%.

Specialist advice could involve many forms of targeted support or intervention such as educational or behavioural programs. Adult safeguarding involves a referral to the appropriate experts who can support the individual's needs such as social care, health professionals and or legal advice.

Response

Disruption performance has decreased, however overall, is reporting above the benchmark. This decrease was expected as outlined in the Q2 pack as the NPCC Serious and Organised Crime portfolio and national leads reset expectations around reporting across all of the Serious and Organised Crime landscape to ensure consistency in recording nationally which previously had been unreliable.

This decrease may continue in to Q4 as new normals are established aligned to the reporting change however operational activity is still on-going with Op Callback 2 data still being analysed, this will lead to an increase in disruptions being reported in Q4 aligned to this specific operation alongside Op Henhouse which is due to take place in February and has previously resulted in significant volumes of disruptions.

Fraud

Proactively Pursue Offenders

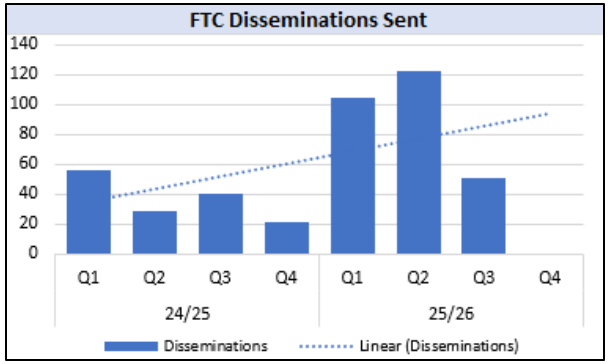
Performance Measure 3: We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in NECC led fraud intensifications throughout the year.

Performance Measure 4: We will support and assist the national development and implementation of the Fraud Targeting Cell by contributing resource and supporting the delivery of systems and processes. We will increase intelligence packages into the system leading to increased proactive operations

Success Measures:	FYTD Performance	Data Trend
F3 Engage in all intensification efforts and target led national operations and evaluate operation-specific outcomes		⇧
F4 Increase the number of Fraud Targeting Cell (FTC) packages allocated, adopted, and investigated		⇩

F3 In Q3, **Op Callback 2** took place, this was an 8-week intensification focusing on courier fraud which is a form of deception in which offenders impersonate trusted authorities to manipulate victims into handing over valuable items to a courier. This operation was a joint operation working alongside the Metropolitan Police. Currently data is being analysed but the Metropolitan Police have reported 33 arrests, 9 subjects charged, 61 serious and organised crime disruptions and £55,000 in cash seized. This intensification also provided links to two other on-going operations involved in courier fraud, identifying two distinct modus operandi involving courier fraud.

Op Tonic took place from 29th September – 5th October. This was a one-week Romance Fraud intensification initiative, for "World Romance Fraud Scam Prevention Day" on the 3rd October 2025. The primary aim was to raise awareness, deliver protect advice and encourage reporting of romance fraud. This also involved collaboration and joint working with Barclays fraud and scam vans in engagement days. This intensification reported 2,299 posters distributed nationally, 12 engagement days, 61,142 impressions recorded on Facebook by Report Fraud and 405,516 social media impressions reported from forces. Overall, given the short timescale and limited resources, the fraud network pulled together collaboratively to promote romance fraud awareness on a national level. They delivered some great events and engaged with the public successfully.



F4 In Q3 a total of 51 disseminations were sent by the Fraud Targeting Cell (FTC). This is a 58% decrease (-71) compared to Q2 of 24/25, and a 28% increase (+11) compared to the same period for the previous year. The main driver for this due to the significantly higher number of disseminations that were sent out as part of Operation Barton in the previous quarter.

There have been several great outcomes for FTC for this quarter such as Op Barton which resulted in 2 moderate disruptions and 31 criminal investigations. In September, Op Lily produced 9 additional subject profiles and following these disseminations, 6 subjects have been interviewed with visits upcoming for the following 3 subjects.

Response

Intensifications

In Q3, Op Henhouse 5 is set to take place in February. This will see coordinated pursue and protect activity across all 43 police force PSNI, Police Scotland, every regional organised crime unit, Trading Standards, FCA and NCA, SFO and Insolvency Service.

This year we have £880K committed for operations across all 43 forces, PSNI, Police Scotland, every region and across Trading Standards, FCA and NCA, SFO and Insolvency Service. CoLP are also leading on an intelligence lead operation with FTC and private industry threat intelligence taking action against 10 UK centric fraud enabling telegram channels. These groups have circa 30,000 members sharing compromised data, tools and tradecraft, benefiting from the anonymity such platforms provide to enable hundreds and thousands of frauds against UK victims.

FTC

Progress on Op seraphim has been made with intelligence products relating to cybercriminals advertising fraud enabling products on Telegram channels. Currently work is on-going with Nigerian law enforcement and the Proactive Economic Crime Team (PECT) network. Close work is also on-going with the Cyber Defence Alliance to identify and attribute the cybercriminals.

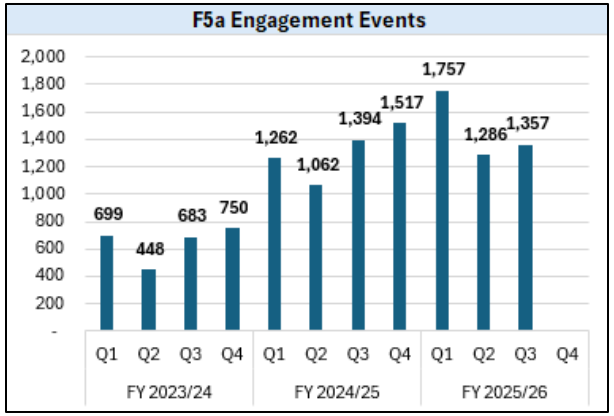
FTC alongside Rick Nolan and the PECT Coordinator, have been having discussions with Flashpoint, a Cyber Threat intelligence company, around assisting in the attribution of the entities to cybercriminals.

Fraud

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

Performance Measure 5: We will develop and deliver a centrally co-ordinated National Fraud PROTECT Network that will align with the National Cyber PROTECT Network, share best practice, and promote local delivery of national messaging.

Success Measures:	FYTD Performance	Data Trend
F5a Increase the number of Protect engagement events and attendees		⇧
F5b Percentage of protect engagement event attendees satisfied with the engagement they attended		⇧
F5c Percentage of protect engagement event attendees likely to change their behaviours as a result of engagement		⇧



F5a For Q3, **1,357 engagements** were held across the network, with **245,507 attendees**. Q3 is reporting a 6% (+71) increase in comparison to the previous quarter and a 3% (-37) decrease on Q3 24/25.

F5b&c The fraud protect surveys continue to be adopted by the national Fraud Protect Network during their presentations, events and interactions with citizens and businesses across the country.
In FQ3, **96%** were very satisfied and satisfied with the event/engagement (2% decrease from Q2)
97% were likely to change their behaviour or already undertake that behaviour (2% decrease from Q2).

In Response
The network continue to utilise the fraud protect surveys during their presentations, events and interactions with citizens and businesses across the country to understand engagement impact. The National Lead for Protect and the Home Office have emphasised to the Regional Coordinators how important they are. Staff consistently receive high praise from attendees for the quality of information shared, and their delivery.

In Q3, as part of **Op Tonic**, Report Fraud Protect Services coordinated a partnership with Barclays who have a fleet of vans that go to various locations to provide banking services to the community, these also offer mobile fraud awareness sessions. During the romance fraud intensification week, several protect officers from various regions joined the Barclays staff in the vans to promote romance fraud awareness (as well as general fraud awareness).

In October, for **Cyber Security Awareness month**, the Protect team focused on promotion of a promotional video in partnership with Meta on 2 Step Verification. The social media campaign reached over 300,000 people with 637,904 impressions.

The **Online Shopping Campaign** launch on the 24th November to help the public to shop safely online. This campaign was done in partnership with the National Cyber Security Centre and Stop Think Fraud aligned to the black Friday shopping events and the online shopping increase during the festive period.
The Online Shopping Campaign reached over 1.7 million people across the UK with 2.8 million impressions. The social media assets were used 114 times by partners and polices forces.
The Action Fraud Parr of the Online Shopping Campaign had over 300,000 impressions and 2,000 reactions across Instagram, Facebook and X.

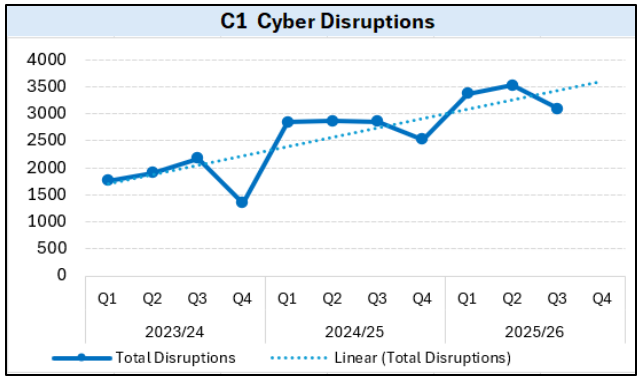
For Q4, the Protect team will be collaborating with SWROCU on proactive romance fraud and victim protect notifications.

Cyber

Improve Outcomes for Victims

Performance Measure 1: We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages. We will ensure full and timely compliance from forces to record disseminations from the NFIB appropriately and that subsequent outcomes are reported back to NFIB correctly.
Performance Measure 2: We will increase intelligence led proactive operations and self-development operations regarding Computer Misuse Act offending, ensuring the relevant deconfliction safeguards are followed.

Success Measures:	FYTD Performance	Data Trend
C1 Increase the number of disruptions against cyber crime		⇧
C2 Increase the number of operations involving the Computer Misuse Act (CMA)		⇩



C2. For Q3, there have been no Vulnerability Notification Packs and Malicious Notification Packs (that informs an organisation about potential weakness in its systems or an alert of malicious behaviour detected on the network such as attempted intrusions) distributed to national and regional Cyber Crime Units.

C1. In Q3, there were a total of 3,089 disruptions.

- 7 major disruptions - 600% increase (+7) in comparison to Q2 25/26
- 75 moderate disruptions - 17% increase (+11) in comparison to Q2 25/26
- 3007 minor disruptions - 13% decrease (-459) in comparison to Q2 25/26.

In comparison to the previous quarter (Q2), Cyber disruptions are reporting a 13% decrease (-442). In comparison to the same quarter for the previous year (Q2 24/25), there has been an 8% increase (+231).
For the Q3, disruptions are reporting 20% (+1,680) above the benchmark, although Q3 reported a reduction is disruptions, overall disruptions have been increasing year on year and are on an upward trend.

The top 2 disruption types are specialist advice at 66% and safeguarding at 16%. Specialist advice could involve many forms of targeted support or intervention such as educational or behavioural programs. Adult safeguarding involves a referral to the appropriate experts who can support the individual's needs such as social care, health professionals and or legal advice.

Under the title Project Capstone, the NPCC Cybercrime Team continues to progress its partnership working with several private sector partners, developing intelligence opportunities to identify UK based cyber criminals and those utilising cyber enabled tools and cryptocurrencies in furtherance of their criminal activities. Q3 25-26 has seen 20 additional intelligence packages disseminated to the ROCU & Proactive Economic Crime Teams (PECT) network. All packages have been accepted by the network and are currently under development. A formal tasking and feedback process continues to be formalised with ROCU leads. Q3 reported seizures more than £1 million of various cryptocurrencies from across the ROCU networks.
During Q3, Project Capstone shared its methodology with Report Fraud and worked collaboratively to identify viable suspects and investigative leads at scale for forces and regions.

Response

Overall, the number of major and moderate disruptions has reduced in 25/26 compared to the same period 24/25. The only strand to see a national increase is Prepare. Individually and reversing this trend is the Northeast ROCU who've seen a significant increase in Protect disruptions during 25/26.

This rise stems from OP ANZAC, a regional project that proactively uses Police Cyber Alarm to identify cyber threats actively posing a risk to businesses. These police interventions prevent potential network intrusions, data exfiltration, and system compromise.

The NPCC Serious and Organised Crime portfolio continues its review of APMIS consistency across all SOC (including fraud and cyber) recorded disruptions which is impacting disruptions recorded as has been highlighted in other pages.

The restructure of the Network, to consolidate the CRC and bring under the direct leadership of the NPCC National Cybercrime Team has been a focus this quarter an d has impacted referral mechanisms and subsequently operations page 12 covers this in greater detail.

Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

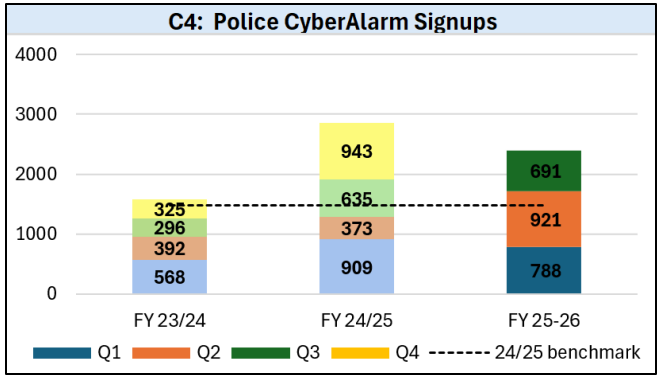
Performance Measure 3: We will develop the current PROTECT notification processes to ensure a consistent approach to both the direct PROTECT officer taskings and the notifications delivered at scale.

Performance Measure 4: We will ensure ROCUs and Forces are regularly using Police Cyber Alarm to help support member organisations when issues are identified and use the data to inform and drive PROTECT, PREVENT and PURSUE activity. PROTECT Officers will promote Police Cyber Alarm to all SME organisations they engage with.

Success Measures:	FYTD Performance	Data Trend
C3 Increase PROTECT notifications issued to victim organisations.		⇧
C4 Protect Officers to promote Police CyberAlarm to SME organisations.		⇧

C3 A Protect Notification is a method used to notify victim organisations when intelligence is received indicating a cyber crime has occurred or is likely to occur against their IT system. If the intelligence suggests a live cyber security threat where quick time actions are needed, then it will be treated as urgent and TICAT will deliver the notification via phone, or via the Protect Network for a same day in-person visit to the premises.

During Q3, the network reports 105 disseminations, of which 103 (98%) were completed within the quarter. Of the Q1-Q3 25/26 disseminations, 49% related to ransomware and 27% a data breach; the main industries tasked out to were Retail/Trade, Manufacturing, Information and Communication, and Financial and Insurance.
Protect Notification outcomes are captured, helping to improve the recording of cybercrime in the UK and quantify the impact of the Protect network; 37% of the Q1-Q2 25/26 taskings have confirmed incidents and crime reports raised.



C4 In Q3 25/26, 691 Small to Medium-sized enterprises (SMEs) signed up to Police CyberAlarm. This is a 25% decrease (-230) in comparison to Q2 and 9% increase (+56) in comparison to the same period for the previous year (Q3 24/25). Overall, performance is reporting 12% above the 24/25 benchmark (+255).

Response

Police CyberAlarm (PCA) is undertaking a change of vendor to Waterstones Ltd. The PCA focus is on delivering a seamless transition, which is likely to negatively impact the drive to increase member sign-ups as capacity is reduced to facilitate this transition work. As a result of this change, several functionalities within the system have been disabled within the current system a transition is planned from the old system to the new system.

As a result of this change, several functionalities within the system have been disabled within the current system a transition is planned from the old system to the new system.

Waterstons Ltd are developing a brand-new, custom-built system for Police CyberAlarm which will deliver improved and increased functionality. The new system is expected to be launched in Q1 of 2026-2027. However, until this available, one of the functionalities that has been disabled are Notification Packages for law enforcement. Member organisations are still able to register, download, install and configure the current system which enables them to receive their monthly threat and vulnerability reports.

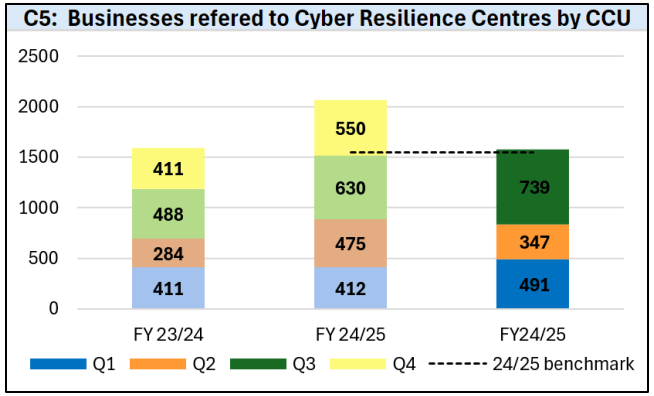
Active promotion of the current version of Police CyberAlarm has ceased until we move closer the launch of the new system, alongside the new system will be a new public facing promotional website and Customer Relationship Management (CRM) solution.

Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

Performance Measure 5: We will deliver the new NPCC Cyber Resilience Centre (CRC) Model. This includes the new Operating Model to deliver the levels of consistency and assurance required. CRCs and PROTECT officers will work together to support each other's work and grow CRC membership

Success Measures:	FYTD Performance	Data Trend
C5 Increase the number of Cyber Crime Unit referrals to Cyber Resilience Centres		⇧



C5

In Q3, the number of Cyber Resilience Centre (CRC) referrals increased by 113% (+392) in comparison to the previous quarter.

Referrals have also increased by 17% (+109), in comparison to the same quarter for the previous year (Q3 Q4/25). Overall, figures are reporting 2% (-26), under the benchmark for this quarter, however Q3 is the highest quarterly reporting month to date.

Response

The restructure of the network, to consolidate the limited companies and bring under the direct leadership of the NPCC National Cybercrime Team was delayed, but is now nearly complete, with the final two regional CRCs expected to close and transfer assets in January 2026. The new operating model, strategy and national delivery plans have been implemented, with regional CRCs creating a regional plan to deliver on the strategic objectives, alongside local priorities. The new KPIs for the network are under consultation with key partners, but are likely to be:

1. Membership growth (particularly in priority sectors)
2. Number of 30 minute 'cyber health checks' completed
3. Number of referrals to, and engagement with, the NCSC Cyber Action Toolkit (CAT)
4. CRC members taking up Cyber Essentials/Cyber Essentials +
5. Conversion of membership to Cyber PATH services

One of the CRC Network's new strategic objectives is integration with Cross-Government SMO cyber resilience projects and initiatives; this is reflected in two of the KPIs also being NCSC priorities. The CRC Network was one of the top three amplification routes for the CAT, following its rollout in October 2025. A new performance framework and leadership structure, alongside improvements to the CRM, will enable the network to drill down into the underlying metrics, and focusing not just on headline numbers, but on demonstrating behaviour change.

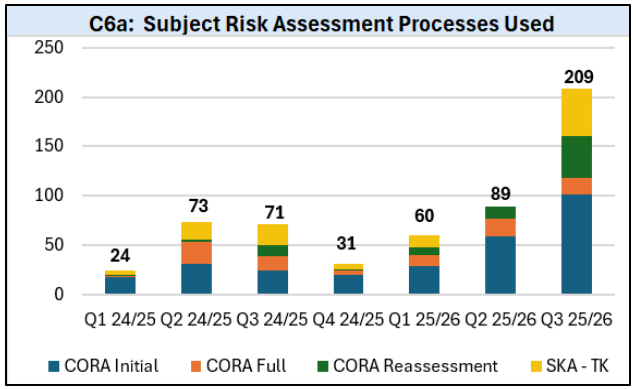
A significant change for the network post-restructure, is the provision of fully-funded Cyber PATH services to SMOs (previously provided at a cost). A campaign to promote the services will commence in January 2026.
Membership as of 31st December 2025 is 29k, with 16 National Ambassadors supporting the network.

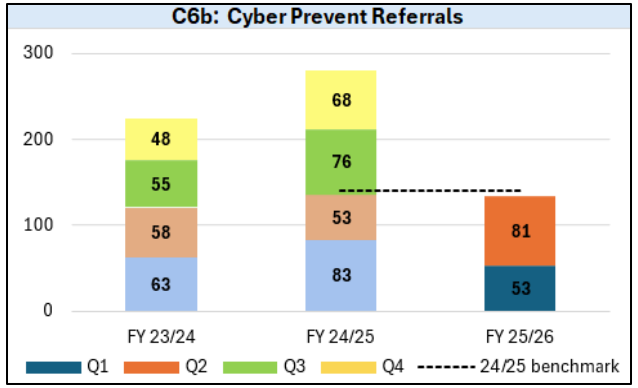
Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

Performance Measure 6: We will develop improved referral process for new nominals - to include Target Operating Model and definition of when a referral should be made. We will introduce a single national or regional referral mechanism and implement risk assessment (CORA) and tasking mechanisms for PR EVENT referrals.

FYTD	FYTD Performance	Data Trend
C6a Increase the number of CORA assessments made		⇧
C6b Increase the number of PREVENT referrals		⇨





C6a A CORA assessment is used to assess the risk posed by individuals referred and helps determine the level of cyber capability from skills, knowledge, and access to technology. This helps decision making in deciding the appropriate intervention, diversion, or support to proceed with. For Q3, risk assessments have increased by 135% (+120) in comparison to Q2 and by 194% (+138) compared to the same period for the previous year (Q3 24/25).

A key focus for CORA in 25-26 is the completion of an assessment at the end of an individual's participation in the Cyber Choices Programme. A dashboard is in the process of being built to measure the impact of interventions on individuals, as a result those that are most effective in reducing risk can be identified.

C6b A total of 77 Cyber Prevent referrals were received in Q3, an 8% (-7) decrease from Q2 and a 1% increase (+1) from the same period for the previous year (Q3 24/25). Overall, Q3 is reporting 2% above the quarterly benchmark year with a total of 215 referrals for the FY 2025/25 to date.

Response

Cyber prevent teams have been reduced due to reprioritisation by the Home Office and funding reduced in 25/26. Whilst the reduction in capacity to deal with referrals reported a downturn in Q1 and Q2, referrals are now on par and have increased for Q3.

Relationships have been strengthened with Counter Terrorism (CT) and the Home Office with a formalising the roles & responsibilities for cross cutting themes. This is important as Counter Terrorism Prevent remains the network's second-largest source of referrals after schools. Formal guidance has been issued to the Cyber Prevent Network to create and standardise existing processes, ensuring Counter Terrorism and Cyber risks are appropriately managed, documented, owned and relationships clear.

Pre and post CORA interventions are now being completed to support evidence on the effectiveness of CORA and Cyber Prevent General.

The Network has had a several Prevent Managers' Governance Meetings, since September 2025, which have been chaired by the NPCC. This is to provide accountability and support to managers in relation to Prevent. This has paramount with regards to increasing the number and quality of the referrals and to share good practice.

The Network continues to run online CPD events for both managers and practitioners on the current risk and threats along with good practice. There are also opportunities for the network to attend session to get briefings from senior leaders and for them to answer questions

Deputy Commissioner Adams and DCI Catney had a meeting with Baroness Browning at the House of Lords in January 2026. Whilst the meeting was about our people in the Network, especially neurodiversity, she asked about Prevent. It was to explain how the Cybercrime Network operates and how we divert people away from cybercriminality. Baroness Browning was impressed and has asked for an additional meeting to discuss Prevent and the Cybercrime Network's people strategy.

Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

Performance Measure 7: We will roll out the Cyber & Digital Specials & Volunteers (CDSV) Programme and platform to every region and Force and ensure effective management and utilisation of CDSV skills across the network.

FYTD	FYTD Performance	Data Trend
C7 Increase the number of CDSV Programme participants and their utilization across the network.		⇧

C7 For Q3, there are currently 146 volunteers on Assemble, across 35 teams. The full time National Lead and Deputy Lead roles now filled, awaiting completion of vetting to start on secondment with CoLP. Formation of cadre of volunteers to work nationally in support of the Lead and Deputy Lead's strategy and delivery.

In Q3, Volunteers logged 1,189 hours of work. This is known to under-represent the true value as volunteers are not always logging their activity. A key element of the new delivery plan is to understand the barriers to recording activity and to develop a more robust way of monitoring performance. a North Wales Special Constable won the Lord Ferrer's Award for his contribution to the Cybercrime Unit and wider force, and a WMROCU volunteer came third in the Team Cyber UK Capture the Flag event.

Volunteers progressed projects to develop a network monitoring tool for domestic abuse victims, an effective radio frequency survey tool and a mapping web app. They supported CCUs at numerous protect engagements and cyber escape rooms. They undertook dark web monitoring and intelligence generation, intel analysis on money mules and cyber incidents, OSINT to secure high risk stalking victims online and progressed their own cyber work files. They supported frontline teams with ethical hacking, using Excel and understanding AI. Volunteers supported the CRC Network through business engagement, and PCA through threat report analysis and consultation around the new supplier specification.

Response

Work has started on a rebrand of Cyber Digital Specials and Volunteers (CDSV) network to reflect wider scope beyond cyber, to the Specialist Crime Volunteer Network. The team is working with the NPCC Science & Technology team and Regional Science & Innovation Managers to embed the use of volunteers within the NPCC strategy. The volunteers' skillsets and current work in the tech-facilitated abuse threat area are also of interest to the National Centre for VAWG and Public Protection.

A phased approach to the expansion of Assemble (volunteer platform) is being scoped by PA Consulting (as part of the NPCC Science & Technology in policing profession project).

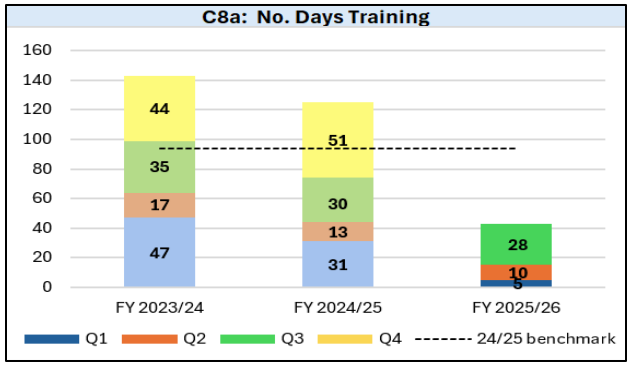
This presents an exciting opportunity for additional support/resource to the volunteering programme. A SWOT Analysis of the platform is underway, gathering user feedback and business need. PA Consulting are keen to explore the potential of piloting Corporate Volunteering, with interest currently from Lloyds Bank and the Institute of Chartered Accountants of England and Wales.

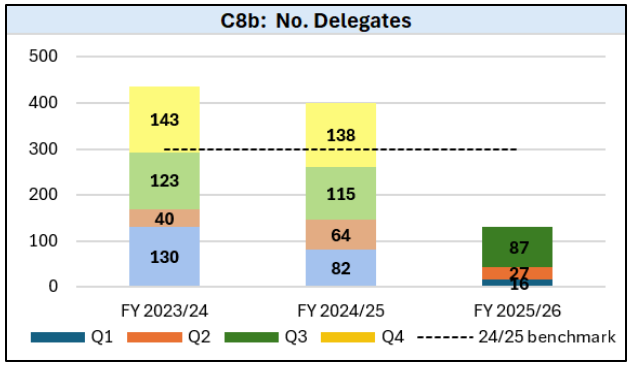
Cyber

Improve Outcomes for Victims

Performance Measure 8: We will revise and roll out a clear training, CPD and accreditation pathway for all roles within TCUK, with regular reviews of the training needs analysis and advancements in technology / threats. NPCC Deliver new strategy and delivery with the Economic and Cybercrime Academy.

Success Measures:	FYTD Performance	Data Trend
C8a Increase the number of Cyber training days		⇩
C8b Increase the number of Cyber training delegates		⇩





C8a For Q3, there has been a 180% increase (+18) in the number of formal training days provided in comparison to Q2. In comparison to the same quarter for the previous year (Q3 24/25), there has been a 7% decrease (-2). Q3 is reporting 38% below the benchmark (-11). Q3, although reporting below the benchmark, delegates and training days have both reported large increased in comparison to Q1 & Q2.

C8b During Q3, 87 delegates were delivered formal training courses, this is a 222% increase (+60) in comparison to Q2 and a 24% decrease (-28) when compared to the same period for the previous year (Q3 24/25). Overall, Q3 is reporting 57% under the benchmark (-169).

Sudocyber	Labs Completed
Oct-25	524
Nov-25	334
Dec-25	552
Total	**1,410**

Response

There was a delay in the implementation of the training programme due to the budget not being finalised by the Home Office for Q1, it was started during Q2, before maximising the number and range of courses in Q3/Q4.

It was decided that courses would be released for the entire year rather than quarterly as previously done. This allows managers in the network to be more flexible with their budgets and when staff attend. The courses have also been delivered (where appropriate) in the North of the country.

A cyber incident response course was developed with the training provider and the NPCC. The course is tailored for the police and allowed practitioners and managers (SIOs) to take part on the same course, but learning their role in an incident. Both groups would be brought together at regular intervals to enhance the learning. This provided staff with the skills and knowledge, whilst at a more cost-effective price than outsourcing it. The feedback has been positive and is now part of the suite of national courses offered.

The NPCC is running a tendering process for training courses for 2026/27 and beyond.

SudoCyber has been running a Capture the Flag (CTF) Exercise in partnership with the NPCC to engage better with the users in the cybercrime network. This resulted in a grand final in Cardiff. SudoCyber will be putting on additional CPD events in 2026.