
BSides
LANCASHIRE

torq

dishMCR

Powered by BARCLAYS | Eagle Labs

cyberlab

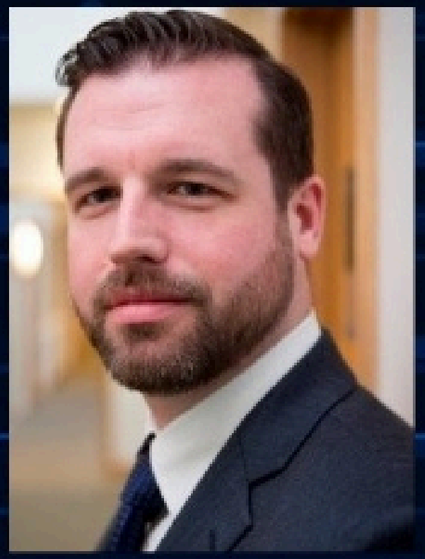
AJBell

AKIMBOCORE
UNRIVALLED PENETRATION TESTING

Lancaster University

Thank you to all our sponsors for making BSides Lancashire 2026 possible!

Jen McCulloch: Co-Founder



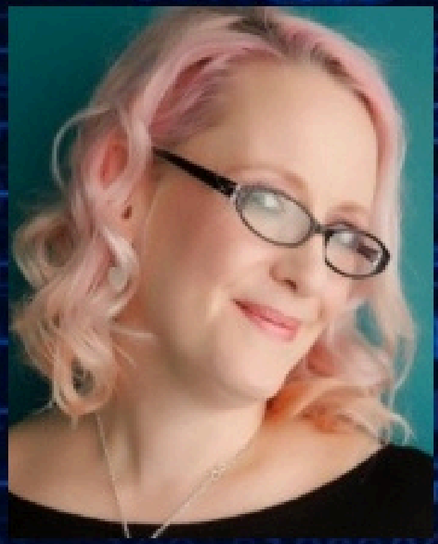
Dan Prince: Co-Founder

Rosie Anderson: Co-Founder

Holly-Grace Williams: Co-Founder

Mike Somers: Co-Founder

Sean Atkinson: Co-Founder



Sam Swift: Head of Commercial

Welcome to the Heart of the North West's Cyber Community

Lancashire has a strong and established security communityand an ever-growing complement of businesses andconsultancies working in the security space.

The North West Cyber Corridor is well-established, so it makes sense to have a BSides community in the NorthWest.

Lancashire

We can’t tell you everything… but this region matters

More Than Scenic Hills

BSides Lancashire sits at the centre of one of the UK’s most dynamic cyber regions.
Anchored at Lancaster University - a global leader in cyber security education and research - the event connects technical experts, students, and industry leaders from across the North West and beyond.
The region’s mix of universities, start-ups, defence-linked innovation, and established tech companies gives BSides Lancashire its own unique edge: serious cyber expertise, delivered with Northern warmth and wit.
Each year, 250–300 people join us for talks, workshops, panels, and hallway conversations that spark ideas, careers, and collaborations.
From local talent to global brands, everyone’s here for the same reason - to share knowledge, challenge assumptions, and build a stronger community.
If you’re serious about supporting the UK’s cyber future, it’s happening right here - and we’d love you to be part of it.

300
Attendance Capacity

SOLD OUT
Every Year

BSIDES: No suits. Just ideas that matter

The World's Favourite Unconference

The Origin Story

Born in Las Vegas in 2009, BSides began when talks were rejected from DEF CON — and the rejected speakers decided to host their own conference instead. That spirit of *DIY rebellion* has since spread to hundreds of cities around the world, from Austin to Athens, from London to Lahore.

Global Reach: Global Community

There are now 700+ BSides events globally, powered by volunteers and supported by companies that care about community.

Each event is unique — shaped by local culture, hosted by local experts, and united by one belief: *Security is everyone's business.*

The Spirit of BSides

At BSides, we:

- 🧠 Share knowledge freely
- 🤝 Build real connections
- 💥 Break things to make them better
- 🛠️ Celebrate curiosity, not corporate buzzwords

Why Lancashire?

BSides events are run **by the cyber community, for the cyber community**. No suits calling the shots. No paid speaker slots. Just pure, grassroots knowledge-sharing, mischief, and innovation.

Who is in the Room?

You'll find everyone from **students and mid-career practitioners** to **security consultants** and **CISOs**. Technical deep dives mix with leadership panels. There are **themed villages,** buzzing with energy — a perfect place to spot top talent or show future hires your community credentials.

A New Space for Fun Times

Because everyone loves Space Invaders!

This year, BSides Lancashire steps into new territory: the West Pavilion at Lancaster University Management School.

It's bright, contemporary, and designed for collaboration — a fitting stage for the conversations and connections that shape the region's cybersecurity community. Some might say it's a culture clash: management meets the creative curiosity of security practitioners. But really, it's perfect: we get to use their cool building!

For our sponsors, the setting offers state-of-the-art facilities, excellent accessibility, and a visually stunning environment that reflects the quality of your brand.

The West Pavilion's open atrium, flexible lecture theatres, and breakout spaces ensure every talk, workshop, and conversation happens in style — and that your presence shines within a professional yet energised atmosphere.


Workshops
Lecture Theatre 16
WP A020
Cloakroom
WP A023
WP A018
Lightning Track
Lecture Theatre 15
WP A015
WC (Gender Neutral)
Thunder Track
Lecture Theatre 18
Accessible Parking
WP A003a
WC (Gender Neutral)
Management School
Villages
Lecture Theatre 14
Registration Desk
WP A036
WP A037
WP A039
Main Entrance
CR20a
A124/A125
A122
Quiet Space
Lecture Theatre 3
CR18
Lecture Theatre 2
Green Ln
Bus Stop - Management School


torq
AKIMBOCORE
UNRIVALLED PENETRATION TESTING
cyberlab
dishMCR
Powered by
BARCLAYS
Eagle Labs
AJBell
Thank you to our sponsors
Lancaster University

Torq is the enterprise-grade AI SOC platform that combines adaptive agentic insights and automation to triage, investigate, and remediateyour most critical threats.

Torq is the enterprise-grade AI SOC platform that combines adaptive agentic insights and automation to triage, investigate, and remediate your most critical threats. Torq streamlines every step from alert through fix. The platform analyzes your risk context to reveal your biggest risks. Working alongside your SecOps staff, the Torq platform integrates with your security stack to facilitate containment and remediation workflows.

We're bringing together experts in digital and cyber security from the public, private and academic sectors to help Greater Manchester's digital security startups to innovate and grow.

Akimbo Core is a UK-based cybersecurity company that specialises in penetration testing, cybersecurity training, and consultancy services. Our team of experts help organizations large and small all around the world to enhance their security posture through comprehensive testing, tailored training, and strategic consultancy. We are particularly known for our bespoke approach to each client's needs, ensuring that our services are aligned with specific security requirements and goals. We offer a range of penetration testing services, including web application, infrastructure, cloud security, wireless network, and firewall security reviews. These services provide detailed assessments and actionable insights into potential security risks. The Akimbo Core team have tested everything from satellite systems to critical medical reporting software to large-scale, national, point-of-sale installations. New challenges are always welcome.

torq

dishMCR

Powered by BARCLAYS | Eagle Labs

cyberlab

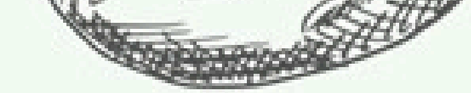
Lancaster University

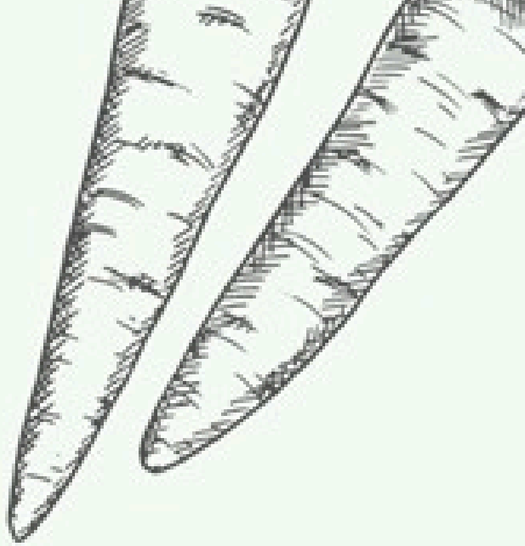
We would like to say a huge thank you to our event sponsors!

Scan the QR code to see the schedule

AKIMBOCORE
UNRIVALLED PENETRATION TEST NG

AJBell





Hot Fork Lunch Menu

served from our hotplate

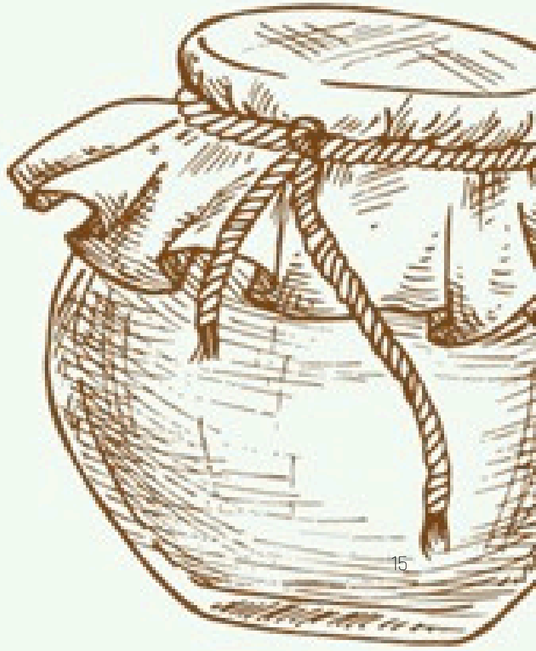
Vegetarian hotpot (V)(VG)(GF)(DF)

Traditional Lancashire hotpot (GF)(DF) Served with crusty bread, seasonal vegetables, red cabbage and pickled onions

Mini cakes

Bowl of fresh fruit

Tea, Coffee and Orange juice



(V) Vegetarian, (VG) Vegan, (GF) Made with Gluten-free ingredients, (DF) Dairy Free

Please note our kitchens handle all major allergens.

If you have an allergy or food intolerance,
please speak to a member of our team.

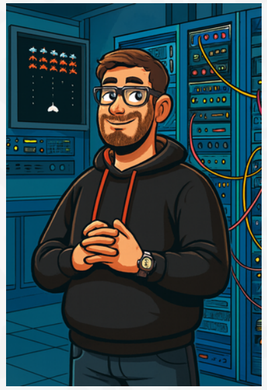
THUNDER STAGE SCHEDULE

Rob Black
10:00 Keynote

Jenny Lam
10:30

Pete Neve
11:30

Ugochukwu Njubigbo
12:05



Aaron Kelly
12:40

Laurie Ibbs
14:15

KN2
14:50

Kinga Kaiserin
15:25

Richard Vaughan
16:15

LIGHTNING STAGE SCHEDULE

Ellie Ball
10:30

Andrew Lucas
10:50

Ben Lintern
11:55

WORKSHOP SCHEDULE

10:30
Joe Burton - Shall we play a game?

11:30 NWCSC - The Community Cyber Wargame

Thunder Talk Synopsis & Bios

10:00 Keynote Rob Black

[Rob Black]

Cyber Security - 10 Things I Hate About You...

Rob is the Director of the UK Cyber Leaders Challenge nurturing new cyber talent, a Professor at the University of Manchester, senior advisor to KPMG's International Information Integrity Institute and an Associate Programme Director at Wilton Park (UK FCDO), events host for RANT and the Director of the Global Institute for Cyber Deception.

Rob was also the Deputy Director of the UK National Cyber Deception Laboratory as well as a Lecturer in Information Activities at the UK Defence Academy, teaching on the classified Cyber Masters Programme. Prior to that he spent over a decade working for the British government, in a range of different roles across defence and national security and the last few years of which were in direct support of cyber operations.

He was awarded UK Cyber Citizen of the Year in 2024. Rob is still trying to work out what he wants to do when he grows up but in the meantime finds himself very fortunate to be doing a range of fascinating work with interesting communities.

10:30 Talk Synopsis & Bio

Jenny Lam

Defence is a team sport... no, really. Leveraging sport psychology principles to maximize performance in response readiness

The talk will cover 3 common sports psychology principles, and how they can be applied to cyber incident and crisis response performance. The primary aim is to help the audience understand how to turn a good response team into a great one, with the right focus during readiness activities. For those who don't work in/with response teams, the takeaways can still be applied to all roles under any type of pressure (and if I'm honest, anything in life). The 3 principles are:

1) Training mental focus on the process instead of the outcome - how noise and distraction divert attention from achieving micro-goals, and feelings of frustration are an indicator of when this is happening. Examples of tunnel vision during technical investigations and how to address it.
2) The confidence cycle - promoting and encouraging confidence with a 3-part cycle, and how to re-engage the cycle during setback.
3) The mission (and motivation) / OR team communication (to be decided which one) - more focused on team cohesion and dynamics. Will either focus on intrinsic motivation and team mission. OR effective team communication under pressure (particularly on technical information communication).

I draw on my own industry experiences in the cyber response readiness & exercising space, as well as my time competing internationally (and representing GB) for an amateur sport. The talk will cover the principle at a high level before focusing on tangible examples and takeaways in the context of cyber incident response. The examples may lean towards SOC/operational level/technical response and procedures, but the principles can be applied to all levels and roles.

11:30 Talk Synopsis & Bio

Pete Neve

Director of Information Security at Synamedia

Tags, and TTPs: OpSec Lessons from Graffiti Writers

Graffiti artists and hackers may seem worlds apart, but both thrive in legal grey zones, chase notoriety with anonymity, and obsess over operational security. This talk explores the real-world OpSec tactics used by graffiti writers and draws direct connections to red teaming, pen testing, and physical security for blue teams. Whatever shade of grey your hat is there's a surprising amount to learn from those who bomb walls, not boxes.

12:05 Talk Synopsis & Bio

[Ugochukwu Njubigbo]

From Brand Campaigns to SOC Dashboards: How Marketing Tactics can transform Security Culture

Too often, security awareness is a checkbox, bland, sleepy, and forgettable. But what if we treated security like a marketing campaign?

In this session, I'll share how I leveraged segmentation, rapid A/B testing, and micro-learning design (from my marketing background) to create behaviour change across NHS clinical and support staff. I'll walk you through real message variants that moved clicks vs reporting, pitfalls I encountered (e.g. accessibility constraints, shift patterns) and how we iterated.

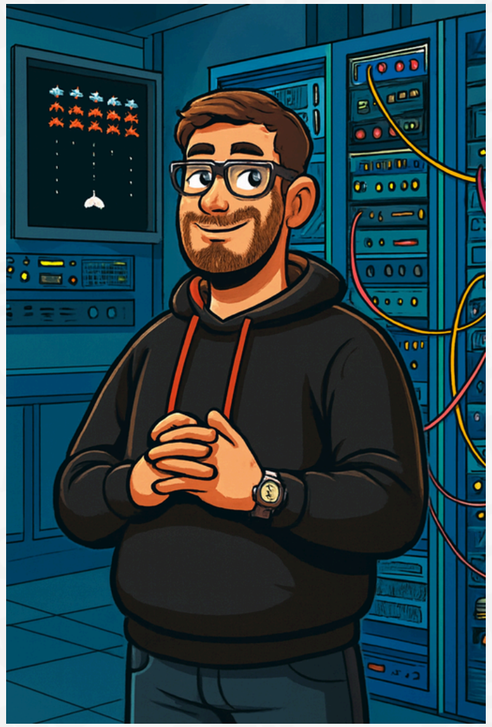
This talk is perfect for SOC leads, security awareness teams, and comms staff looking for low-cost, high-impact ways to shift culture.

This talk will walk you through how I turned marketing playbooks into measurable security culture gains across my recent careeer having recently transitioned from digital marketing to Cyber Security with no big budget required.

Learning Outcomes
- Design a segmented awareness campaign using A/B testing to optimize message impact
- Create micro-learning modules that respect shift schedules and cognitive load
- Measure and communicate behaviour change (click-rate drop, reporting increase) to leadership

My background: I am a Cybersecurity Analyst at the NHS, with a background as a digital marketing lead. I specialise in human-centred security awareness programs. I have crafted campaigns that move behaviour, builds detection strategies under resource constraints, and frame security narratives for both technical and executive audiences.

12:40 Talk Synopsis & Bio



Empowering Organisational Resilience with MS Purview

Throughout this talk, we will be exploring some of the features of Microsoft Purview and looking at how these can be used across various organisations to enable a more resilient business. By looking into feature sets that may have already been paid for but potentially not fully established, we can show some easy wins for all organisations when it comes to GDPR and HMRC records compliance. The tools shown here should then better enable you to go back and implement stronger methods of ensuring the data security of what you are storing and processing, automating some repetitive tasks and enabling easier ways of proving compliance with security standards like ISO 27001.

Aaron Kelly

14:15 Talk Synopsis & Bio

Laurie Ibbs

Vibe Secure! or... why the machine loves you...
(it really really does, like you are the best, high five!)

“Vibe coding” has become a shorthand for everything people fear about modern software development: AI slop, dynamic languages, fast-moving teams, and systems that seem to grow without anyone fully understanding them. It’s often dismissed as insecure and reckless.
This talk argues something different. Vibe coding isn’t the problem. Unchecked freedom is.
Most developers are not careless. They are overwhelmed. They face blank pages, ambiguous requirements, distributed systems that hide intent, and timelines that leave no room for anything but completely accurate estimates. Generative tools and exploratory coding emerged as coping strategies, not moral failures. The real danger appears when these generative approaches are combined with dynamic languages, fragmented microservices, weak contracts, and little to zerotesting. At that point, systems stop encoding intent. Correctness becomes a shrug and a prayer, rather than a technical guarantee.

In this talk, we explore why that combination is uniquely fragile, why “move fast” without constraints becomes indistinguishable from chaos, and why security failures are often the symptom of missing structure rather than bad intentions.
Using a real, evolving Rust graph-modeling project as a concrete example, the talk introduces an alternative mental model: generative freedom followed by algorithmic constraint. First, we embrace exploration to overcoming the blank page, using AI to scaffold ideas, and letting humans think creatively. Then we introduce a hard, non-negotiable rubric: explicit transactions, typed relationships, executable contracts, and invariants that cannot be silently violated. As the compiler enforces correctness, the developer learns more about their craft than code review can provide.
This approach doesn’t slow teams down. It liberates them. When intent is encoded in types, contracts, and relationships developers can refactor, collaborate, and use generative tools boldly, because the system itself pushes back against nonsense, and the skilled developer can spot drift in the architecture. The result is not rigidity, but confidence. Not bureaucracy, but clarity. Not less creativity, but creativity that survives scale, distribution, and time.
This talk re-frames the debate around vibe coding, security, and AI assistance. The future isn’t choosing between freedom and correctness, but designing systems that can support both.

14:50 Talk Synopsis & Bio

Key Note 2

15:25 Talk Synopsis & Bio

Kinga Kaiserin

They Don't Need the AI to Spy on You. Are They, Though?

In light of the plan to roll out the facial recognition in the UK nationwide, in all town centres, the concerns raised the most are how the AI is going to make it potentially wide-reaching, inaccurate or abusive. The UK is one of the most surveilled countries in the world, after all.

However, many don't realise that common technologies, such as radio/WiFi (or even a bag of crisps) can already be used to spy on people. The talk will therefore explore what's already out there. We will also explore what laws are in place that either prevent abuse, or, on the contrary, enable it. We will also see what government agencies and private entities have access to data generated by population surveillance, what safeguards are in place, and how that ties with other legislation, both planned (Data Use and Access bill, digital ID) and existing, such as Online Safety Act and Policing and Crime Act.

The talk aims to both raise awareness about the legal landscape of mass surveillance and what's planned ahead, as well as make people aware of surveillance methods that do not require new technology.

We will also discuss potential counter surveillance methods - and if, in turn, using those is (and will remain) legal. It will also explore how the same techniques the state apparatus may use to spy on the general population for convenience can be used by malicious actors. Finally, we will fact check whether mass surveillance does influence crime and in what manner, so that the attendees can make their own mind about whether the use of such methods by the state is justified, and to what degree.

Tinkering and tearing things apart led me to tech. Tech on the internet informed my security and privacy concerns. Privacy concerns led me to security compliance and cyber. Somewhere along the way, accidentally, it landed me in AI stress testing. My talks reflect the intersection of tech, law, and real-life impact.

16:15 Talk Synopsis & Bio

Richard Vaughan

Red Teaming LLMs: A Practical Guide to Breaking AI Applications

Every major coding assistant violates the same security principle. GitHub Copilot, Windsurf, Cursor, Google's tools - all of them. This talk explains why, demonstrates how attackers exploit it, and gives you a practical framework you can apply to any AI system in your organisation.

The Lethal Trifecta is a simple model: an AI agent becomes critically dangerous when it processes untrustworthy input, has access to private data, and can change external state. Satisfy all three, and a single prompt injection can escalate from a nuisance to a breach. The uncomfortable truth is that most production AI deployments already satisfy all three - and nobody is testing for it.

This session is a practical guide to red teaming LLM applications, drawn from real-world testing and public research into AI agent vulnerabilities. We'll cover:
- The Lethal Trifecta in practice: How to assess any AI system for critical risk in under five minutes, using a framework that executives and engineers both understand.
- Attack techniques that work today: Prompt injection, tool poisoning, MCP supply chain attacks, and cross-agent worm propagation - with real examples from coding assistants and enterprise AI deployments.
- The recursive problem: Why your security testing tools themselves satisfy the Lethal Trifecta, and what that means for safe red team operations.
- What actually helps: Permission architectures, sandboxing strategies, and the Rule of Two - designing AI systems that can't satisfy all three dangerous properties simultaneously.

You'll leave with a concrete assessment checklist, an understanding of the attack surface that most organisations aren't testing, and the uncomfortable knowledge that the AI tools you used this morning are probably vulnerable to everything discussed in this talk.
No prior AI security experience required. Bring healthy paranoia.

Richard Vaughan is the founder of ThreatControl, a security consultancy specialising in AI application security testing and offensive security services. Richard's current research applies the Lethal Trifecta - a framework developed by Simon Willison and Meta's AI security team - to real-world AI deployments. The framework identifies three properties that, when combined, create the highest-impact attack scenarios. His analysis shows that every major coding assistant on the market today violates this principle, this finding shapes both his testing methodology and his advisory work with clients.

ThreatControl's portfolio spans the full security assessment lifecycle: from passive perimeter scanning and vulnerability assessment through continuous monitoring, supply chain risk analysis, and dedicated AI security testing. The company works primarily with SMEs and startups who need enterprise-grade security insight without enterprise-scale budgets.

Security Lancaster | Lancaster University

Lightning Talk Synopsis & Bios

10:30 Talk Synopsis & Bio

To Scan Or Not To Scan? An Investigation into Age-Related Differences in QR Code Tampering Detection By Design

Ellie Ball

QR codes have become an integral part of our digital environments. However, QR codes are vulnerable to tampering, known as "Quishing", which presents a significant threat to user security. This attack is concerning for all users, but especially for older adults who can have difficulties navigating digital interfaces and who can be more vulnerable to technology-based fraud. Research by Bekavac et al. (2024) suggested vigilance to QR code tampering could be improved through the design of QR codes, proposing transparent backgrounds and additional logos make it more difficult for scammers to modify the QR codes and make it easier for users to detect signs of alterations. But there is a lack of empirical evidence of the efficacy of these designs, particularly amongst older adults. To address this, we conducted a controlled experiment to examine how users' scanning engagement behaviour was influenced by these "safer" QR code designs but also by designs mimicking QR code tampering. In total, 129 participants, 65 younger and 64 older adults, were recruited. The task involved displaying six posters, each presenting one of three genuine (standard, transparent background, safe logo) or three fraudulent (stuck over, misaligned, mirrored logo) QR code designs and participants had to decide which to scan. Scanning "genuine" QR codes added points to their total, but scanning "fraudulent" QR codes deducted points. Overall, the findings highlighted that QR code presentation had a significant influence on QR code-engagement behaviour, as users opted to scan the standard QR code significantly more than the other QR code designs. Compared to younger adults, older adults were more likely to scan the fraudulent QR codes, however the difference was not statistically significant. This talk will discuss the implications of the findings for user susceptibility to QR code-based fraud and the success of this approach in the real world.

Ellie Ball is a final year PhD psychology student at Lancaster University, where she studies QR code engagement, looking specifically at QR code security and QR code scam susceptibility. Her work focuses on understanding how users, young and old, are interacting and behaving with QR codes in the domains of attitude, cognition, and behaviour to develop a deeper understanding of the factors that could make individuals vulnerable to QR code scams. QR codes have become an integral part of our digital environments but with that, the prevalence of QR code scams has increased, with Action Fraud reporting that between April 2024 and April 2025, £3.5 million was lost to fraudulent QR codes in the UK alone. Through her research, she aims to improve the efficacy and specificity of future scam intervention plans, to reduce the number of individuals falling victim to malicious QR codes.

10:50 Talk Synopsis & Bio

Andrew Lucas

What Alzheimer's Teaches Us About Security

This talk examines how living with someone with Alzheimer's disease reveals uncomfortable but essential truths about human behaviour that cyber security consistently overlooks. Drawing on the lived experience of caregiving, it challenges the assumption that people are reliably attentive, rational, and capable of following complex security instructions. Alzheimer's makes visible what is true for all humans at times: memory is fragile, attention is inconsistent, stress impairs judgement, and familiarity often substitutes for careful verification. In daily life with cognitive decline, people forget steps they have just been shown, repeat actions they believe are new, and trust routines or familiar cues even when they are no longer correct. The talk draws a direct parallel to workplace cyber security, where users are expected to remember numerous passwords, recognise subtle threats, and behave perfectly while juggling deadlines, interruptions, and emotional pressure. These expectations create predictable behaviours such as password reuse, unsafe shortcuts, and clicking convincing phishing messages, not because people are careless, but because they are adapting to systems that demand more cognitive effort than is realistic. The talk explores how familiarity drives trust, showing how phishing attacks succeed by mimicking routine communications and authority in the same way that a familiar face or voice reassures someone with Alzheimer's, even when it should not. This illustrates why awareness training and calls for vigilance have limited impact, as human brains are wired to rely on recognition rather than analysis, particularly when time is scarce. Stress is presented as a critical factor, with mistakes most likely to occur at moments of urgency or overload, precisely when security controls often become more intrusive rather than more supportive. The talk also highlights the corrosive effect of shame, noting that people experiencing cognitive decline may hide mistakes to avoid embarrassment, just as employees frequently fail to report security incidents for fear of blame or punishment, allowing minor errors to escalate into serious breaches. From these observations, the talk reframes cyber security as a human-centred design challenge rather than a compliance problem, arguing that effective security should resemble good caregiving by anticipating failure with empathy. It advocates for systems that reduce reliance on memory, minimise decision-making, prioritise safe defaults, automate protection wherever possible, and focus on rapid recovery rather than punishment when things go wrong. The conclusion challenges the audience to abandon the myth of the ideal, always-careful user and to accept that distraction, stress, and imperfect memory are normal conditions, not exceptions. The central message is that security systems designed only for people at their best will inevitably fail them at their most human.

11:55 Talk Synopsis & Bio

Zero Trust, Before the Cloud:
What Windows Firewall Got Right Years Ago

[Ben Lintern]

The science is clear. If we keeping setting our bar at “Awareness” we are destined to remain short on our aspirations to strengthen security. This fun, light-hearted 15 minute demonstration explores how we can think “differently” when seeking to communicate and engage people about cyber security.

In the summer of 1973, over eight days, the CIA conducted a series of scientific experiments, in carefully-controlled conditions, to test the ability of an individual use paranormal perception to replicate drawings unseen to them. The CIA’s intention was to explore possible new avenues with which to exfiltrate key intelligence from the Soviet Union.

As a result of the success of the experiment, they concluded that the individual had demonstrated paranormal perceptual ability in a convincing and unambiguous manner. The individual being tested was Uri Geller. Over 50 years on from these experiments, and using declassified original CIA documents available on their website, we seek to recreate that original drawing replication experiment at BSides Lancashire.
Of course, the moral of our story is not that our Information Security systems need urgently updating to accommodate protection from psychic powers. But the presentation does demonstrate that even when tight controls are applied, individuals can be misled through deception and deceit.

Andrew’s path into cyber security is far from traditional. A burning curiosity in multiple diverse subjects led to a combined honours degree and first Masters that was an exercise in procrastination about which path he wanted to follow when he grew up. After 25 years in media and the arts, Andrew subsequently worked in environmental science, politics and the Civil Service. Throughout his career, he led digital transformation, security and culture change projects. Following a second Masters in Cyber Security at Lancaster University,
Andrew worked as a consultant and was subsequently appointed Director of CentriVault. He is also founder and Director of NaturallySecure.Net, a startup which is driving action research into strengthening cyber security behaviours and cultures. Andrew is a qualified teacher and has lectured at colleges and universities. He has always been passionate about seeking creative ways to engage audiences in new learning and experiences. Magic has been a love since childhood. As a teenager, he performed regularly and had a trick published in an international magic magazine. As real life took over, the magic was retained as a hobby and occasionally brought out for, family, friends and colleagues. On working in cyber security, Andrew realised the possibilities of using magic to demonstrate cyber security concepts. It may have also have provided an excuse to spend rather too much money going to magic conventions and buying tricks. He is still intensely curious.

Security Lancaster | Lancaster University

torq

AJBell

Workshop Info

AKIMBOCORE
UNRIVALLED PENETRATION TEST NG

cyberlab

dishMCR
Powered by
BARCLAYS | Eagle Labs

10:30 Workshop

Joe Burton

Workshop: Shall we play a game?

Games and gaming have shaped cyber security culture, practice, and research for decades. In the iconic movie "War Games" (1983) a young hacker hacks into a nuclear command and control system, thinking he's playing a video game. The movie prompted President Reagan to take additional measures to protect US nuclear infrastructure. In more recent times, concerns have arisen over the use of gaming platforms to spread malware and encourage radical and extreme online communities. Research on the intersection of gaming and (cyber) security has been influential, and in teaching and education cyber security 'games' have become a prominent and effective teaching tool to train creative thinkers in entertaining and pedagogically innovative ways.

This workshop brings together a group of 'gamers' at Lancaster University to reflect on their experiences of running and designing games for security and cyber security. It will highlight three pillars of the 'gamification' of (cyber) security – 1.) Games for Skills/Education 2.) Games for Research 3.) Research on Games. In doing so the workshop will explore how games are currently being used at Lancaster to train students in cyber security; how games (including 'war' games) are being used to answer important and complex research questions; and how researchers are studying gaming environments as both a site and playground for security actors. The workshop will begin with a panel discussion (20 minutes). In the second part of the session (40 minutes), the panellists will talk about how to design games for education and research. This part of the session will highlight game design processes, how to create learning objectives, how to link games to research questions, how to conduct post-game analysis and research, and ways to make games fun and engaging.

11:30 Workshop

NWCSC

The North West Cyber Security Cluster is a collaboration of cyber security professionals and experts in the North West region. Our purpose is to support, connect and empower the cyber security community in the North West region by focusing on 3 key areas: Innovation, skills growth, and ecosystem development. Through networking events, knowledge-sharing platforms, and strategic partnerships, we cultivate a supportive environment to encourage innovation and information exchange. We offer free membership to individuals, organisations, and businesses in the North West with an interest in cyber security. The NWCSC is a Not-for-Profit Community Interest Company.

Workshop title: The Community Cyber Wargame - Exercise Kirbymere

Workshop description: Do you have what it takes to navigate a large-scale cyber crisis? This workshop is an interactive, scenario-based exercise that lets you experience what goes on behind the scenes during a major cyber attack.

Using real-life news stories from companies like M&S, Co-op, and Jaguar Land Rover, you'll get a taste of how they navigated their toughest moments. Prepare for a chaotic session that shows that the best defense involves people from every background working together.

As a cyberattack hits your fictitious company, Kirbymere Retail Group, you will work through the critical operational and strategic hurdles that emerge during a real-time crisis. Facing the classic 20-sided dice to represent the uncontrollable elements of real-life chaos, you and your peers will discuss response strategies and decide how you will adapt to the ever-changing situation and no-win dilemmas.

You'll walk away with a deeper understanding of how different roles come together during a crisis, and the inspiration to rethink your own approach to business resilience. No prior technical or cyber knowledge is required—just a willingness to collaborate and share your perspective.

Village Info

Capture The Flag Challenge

Things to know:

- You will need a laptop or desktop computer with up to date version of Chrome, Edge, Safari or Firefox as all challenges are run entirely within the web browser - No VPNs or VMs required
- Points are awarded immediately upon successful flag submission and there will be a live leaderboard
- 11 challenges and 2 hour time limit - 1 challenge requires headphones

CHALLENGES & SCORING

CHALLENGE	CATEGORY	DIFFICULTY	PTS
Port Scanner	Network Recon	Beginner	25
The Curious Web	Web Recon	Beginner	75
Port Probe Protocols	Service Enum.	Beginner	100
Client Brief: Prof. Practice	Legal / Ethics	Beginner	100
Hash Cracker	Cryptography	Intermediate	100
Deepfakes & Dollars	AI Forensics	Intermediate	150
Injection Junction	Web App Sec	Intermediate	150
Windows: NTLM Hash & Crack	Active Directory	Intermediate	150
OSINT Reconnaissance	Open-Source Intel	Intermediate	200
Advanced Chess Gambit	Logic / Crypto	Advanced	200
SOC In The Loop	Threat Hunting	Advanced	250

Link to the challenge will appear on the website **HERE**

A code to join the challenge will be available in the Village Space

Hosted by Cydena

The UK's only cybersecurity talent platform where your skills are verified, not just claimed. Whether you are looking for a new role in cybersecurity or just interested in enhancing your skills and validating your capability Cydena has technical challenges and CTF's to help you in your cyber skills development

Come and get hands on with the Infosec Battle Bots, where creativity combat and engineering come together to create an unforgettable experience.

In the Village Space

Bot or not?

Bot or Not? Real-world detection of AI-generated content

As AI becomes increasingly capable of generating convincing content, this raises significant challenges for law enforcement, online safety, journalism, public trust, and beyond. The Bot or Not? suite of perception tests investigates whether ordinary people can reliably distinguish between human and AI-generated language, speech, and creative content, how they arrive at their conclusions, and how confident they are in their judgements.
[Optional extra stuff but probably not necessary…]

This largescale project combines forensic linguistics and data science, and the findings from these studies provide a range of insights including the limits of human detection and the linguistic features that influence trust and credibility. These insights help identify where AI systems currently succeed in mimicking human communication and where they still leave detectable traces.

The findings have important implications across an enormous array of contexts, from national security through to interpersonal crime through to the integrity of the evidential process and beyond. By improving understanding of how AI-generated content is (mis)perceived, Bot or Not? contributes to the development of more reliable detection tools, better policy responses, and stronger safeguards for digital integrity.

Our Chosen Charity for Sticker Stall

Bowland Pennine Mountain Rescue Team

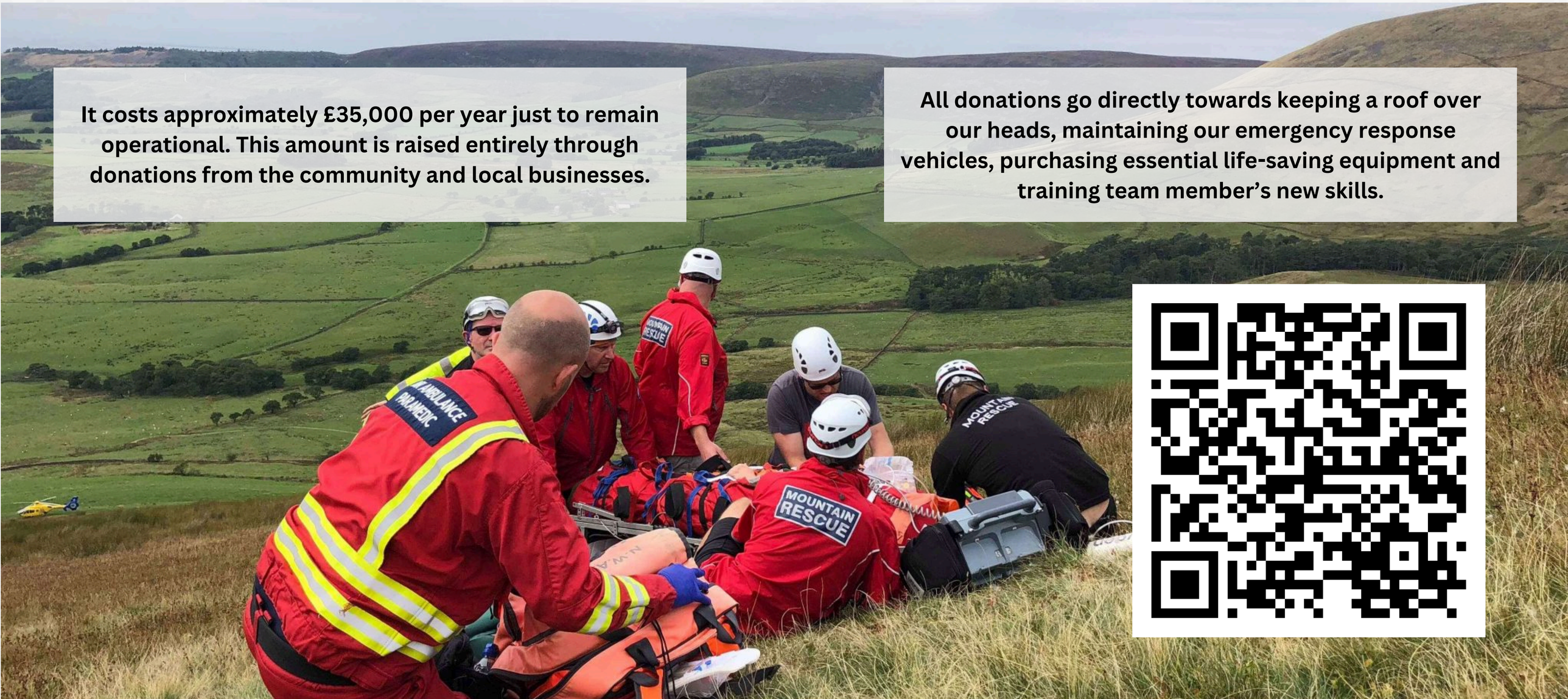
Bowland Pennine Mountain Rescue Team (BPMRT) is a registered charity providing an essential, life-saving emergency service to the people of Lancashire and beyond.

The Team attends an average of 70+ callouts each year and is staffed entirely by unpaid volunteers

Security Lancaster | Lancaster University

Our Chosen Charity

Bowland Pennine Mountain Rescue Team



It costs approximately £35,000 per year just to remain operational. This amount is raised entirely through donations from the community and local businesses.

All donations go directly towards keeping a roof over our heads, maintaining our emergency response vehicles, purchasing essential life-saving equipment and training team member's new skills.

After Party at Barker House Farm
Evening Buffet Menu

Vegetable Kebab (V)(VG)(GF)(DF)
Harissa cauliflower steak (V)(VG)(GF)(DF)
Vegetarian sausage (V)(VG)
Pork sausage (DF)
5oz Rump steak (GF)(DF)
Tandoori Chicken skewer (DF)(LF)

Served with Crusty bread, Peppercorn sauce, Roasted tomatoes and garlic and thyme mushrooms
Roasted corn on the cob with Cajun butter
Mini jacket potatoes
Followed by
A dessert table to include a choice of cakes and cheesecakes
Tea and Coffee


BSIDES
LANCASHIRE