

Northwest Cyber Digi-Tech Network

Meeting Minutes

Date: Wednesday, 19th February 2024

Time: 10:00 AM – 1:00 PM

Venue: Online, Zoom

Facilitator: Mohamed Jaishan, LSCP

1. Welcome and Housekeeping

The meeting commenced with a welcome and housekeeping by Mohamed Jaishan. The agenda was reviewed, and attendees were briefed on the meeting format and expectations.

2. The Risks of Ransomware and AI-Facilitated Criminality – DS Danny Gavin, Merseyside Police

(10:10 AM – 10:40 AM)

Triple Extortion in Cyber Attacks: Insights from Merseyside Police

Danny from Merseyside Police presented on the growing threat of triple extortion ransomware—a sophisticated cyberattack method that combines data encryption, data theft, and third-party pressure. Attackers not only lock victims out of their data but also steal sensitive information and threaten to expose it unless a ransom is paid. To increase pressure, they target third parties such as customers, suppliers, or partners, making recovery even more difficult and ransom payments more likely.

Mitigating Triple Extortion Cyber Attacks

To counter these threats, organizations should follow a multi-layered cybersecurity approach based on the principles of Prepare, Protect, Prevent, and Pursue:

- **Data Encryption & Backup** – Maintain offline, encrypted backups to safeguard data from ransomware attacks.
- **Access Controls** – Enforce MFA (Multi-Factor Authentication) and restrict access to sensitive information.
- **Network Monitoring & Threat Detection** – Deploy intrusion detection systems (IDS) and AI-powered threat monitoring.

- **Employee Training** – Educate staff on phishing, social engineering, and ransomware tactics.
- **Incident Response Plan** – Develop a comprehensive cybersecurity response strategy, including legal and regulatory actions.

The Growing Threat of AI-Driven Cybercrime

Danny also emphasized the rise of AI-powered cyber threats, including deepfake technology for identity fraud, social engineering, and misinformation, making deception more convincing than ever. Additionally, AI-driven brute-force attacks have made password cracking faster and more effective. To combat these risks, organizations should implement AI-driven security solutions, advanced threat detection, and enforce MFA (Multi-Factor Authentication) to strengthen their cybersecurity posture.

Key Takeaways

- Do not pay ransom to cybercriminals, as this funds further attacks.
- Report all incidents to The Merseyside Cyber Dependent Crime Unit, which may provide financial assistance to cybercrime victims.
- By staying proactive and strengthening cybersecurity measures, organizations can mitigate the risks of triple extortion attacks and AI-driven cyber threats.

3. Digital Adoption and Transformation in Regulated Care – Mazz Akhtar, Lancashire & South Cumbria ICB

(10:40 AM – 11:00 AM)

Discussion:

An overview of the ongoing digital transformation efforts within regulated care was provided, with an emphasis on digital safety, compliance, and emerging technologies aimed at improving care standards. It was noted that ensuring **Data Security and Protection Toolkit (DSPT) compliance** and **secure NHS mail adoption** are key priorities for **Lancashire and South Cumbria ICB (LSCICB)**. The discussion highlighted both the challenges faced by care providers and the measures in place to support them in adopting digital solutions effectively.

Key Points Discussed:

Digital Safety and Compliance:

It was highlighted that **DSPT compliance currently stands at 71%**, with a **target of 80% by March 2025**. It was noted that care providers who had not yet registered or renewed their DSPT status were being targeted through a structured engagement plan.

The discussion emphasized the importance of **NHS mail adoption**, noting that many providers struggle with technical and administrative barriers.

Digital Medication Management:

The introduction of **Medy Box**, a **smart medication device**, was outlined as a potential solution for reducing the need for in-person care visits and improving medication adherence. It was noted that the programme aims to support **up to 1800 individuals by December 2025**. The involvement of **Connected Health Systems Ltd.**, which is working alongside ICB to integrate this technology into domiciliary care services, was also discussed.

AI-Powered Fall Prevention & Response:

The rollout of **Nobi AI Smart Lamps** in care homes was discussed as a key initiative to improve fall detection and prevention. It was noted that **500 lamps have been installed across 50 care homes**, supporting **270 high-risk residents**. The technology enables **real-time fall alerts, automated lighting, and resident monitoring** to help caregivers respond quickly and prevent falls. Data from the project showed a **71.79% reduction in falls per 1,000 resident days**.

Challenges & Infrastructure Needs:

The discussion focused on **WiFi limitations** in care homes and the impact on digital technology performance. It was highlighted that **strong, reliable WiFi is critical** for AI-driven solutions like **Nobi Smart Lamps** and **Medy Box** to function effectively. It was noted that addressing **infrastructure gaps** would be a key priority moving forward.

4. Exercise in a Box – James Barber, Jamescape

(11:10 AM – 11:40 AM)

James Barber introduced **Exercise in a Box**, a cyber resilience exercise tool designed to help organizations test their security processes in a safe environment. He also covered:

- **NCSC** – National Cyber Security Centre
- **Security of Cloud Productivity Suites** – measures to take if the organisation was to experience a cyber-attack.

5. PainChek – Amran Sanghera

(11:40 AM – 12:10 PM)

Discussion:

An overview of **PainChek** was provided, explaining its role in **pain identification and assessment**. It was noted that PainChek is a **regulated and clinically validated** digital tool designed to enhance the detection and management of pain, particularly in individuals who may struggle to communicate their discomfort effectively.

The discussion included insights from **Dovehaven**, a care organization that has been using PainChek for the past six months to **identify and monitor pain levels** among residents. It was explained that the tool collects **pain assessment data** to support **chronic pain management** and inform clinical decision-making.

Key Points Discussed:

Implementation and Outcomes:

- PainChek has been in use at **Dovehaven for six months**, providing real-time insights into residents' pain levels.
- The technology has contributed to a **60% reduction in severe pain**, a **40% reduction in moderate pain**, and a **35% reduction in mild pain**.
- The system has also led to a **58% reduction in resident-resident altercations**, highlighting its impact on improving overall resident well-being.

Pain Identification & Assessment:

- PainChek enables **objective pain assessments**, supporting care staff in **recognizing non-verbal signs of pain**.
- The system is particularly useful for residents with **cognitive impairments** or **limited verbal communication skills**.
- Pain data is **integrated into chronic pain management plans**, ensuring that interventions are **data-driven and evidence-based**.

6. SmartSocks: Transforming Dementia Care – Zeke Steer, Milbotix

(12:10 PM – 12:30 PM)

SmartSocks: Revolutionizing Dementia Care with Continuous Health Monitoring

Zeke, the founder of SmartSocks, introduced the innovative wearable technology designed to improve the well-being of individuals with dementia while reducing care costs. SmartSocks continuously collect and analyse physiological data, such as pulse rate and gait, through a WiFi-based cloud backend. The system adapts to the user's behaviors over time, identifying triggers and suggesting personalized calming strategies to minimize medication use, particularly antipsychotics.

The socks integrate with the Abbey Pain Scale for reference and are designed to be discreet and comfortable, significantly reducing the risk of removal compared to other wearables. With ongoing trials in collaboration with universities and care organizations, SmartSocks offer a cost-effective (£40/month) and practical solution, lasting up to 50 washes.

Additional features include integration with other smart technologies like an AI-enabled hug teddy bear and an API for developers. Available in two versions—Comfort and Discovery—and five colors, SmartSocks provide a seamless, non-invasive way to monitor health in real time.

7. Harnessing the Power of MS Automation and Copilot – Sean Tickles, Littlefish

(12:30 PM – 12:55 PM)

The Evolving Cybersecurity Landscape: Generative AI, Threats, and the Need for Proactive Protection

Sean from Littlefish discussed the growing role of Generative AI in both detecting and creating cybersecurity threats. While AI has been instrumental in identifying risks, detection alone is no longer enough—attackers are now leveraging the same technology to develop more sophisticated threats.

To stay ahead, organizations must continuously refine their TTPs (Tactics, Techniques, and Procedures) and shift towards proactive defense strategies. With security teams overwhelmed by constant alerts, automated solutions like automated containment and Security Copilot must become the new baseline for protection rather than reactive measures.

Looking ahead, cybersecurity efforts must focus on improving efficiency and effectiveness, ensuring that security teams are not just keeping up but staying ahead of hackers. Proactive data protection will be key to securing digital environments in an era where threats are evolving faster than ever.

Littlefish provides Managed IT Services tailored to businesses' specific needs, enhancing overall performance. Their Cyber Security Services offer intelligent protection against evolving threats, empowering teams to operate securely. Additionally, their Cloud Solutions enable centralized management with flexible, anytime-anywhere access, ensuring smart and adaptable business operations.

8. LSCP Updates

(12:55 PM – 1:00 PM)

- LSCP provided updates on **Cyber Security Awareness & Data Protection training**.
- Ongoing support for **DSPT compliance and digital audits**.
- A **Zoom Poll** was conducted to gather feedback and discuss future network improvements.

9. Next Meeting Date

The next meeting is scheduled for **Thursday, 22nd May 2025 (10:00 AM – 13:00 PM, Online)**.

Meeting Adjourned at 1:00 PM.