Northwest Cyber Digi-Tech Network

1. Welcome and housekeeping - Ann Garvey, Key Account Manager – LSCP

The network began with a welcome and housekeeping from AG. The agenda was read, and the floor opened for the first speaker, Danny Gavin.

---

2. Cyber Fundamentals and Cyber Hygiene - DS Danny Gavin(DG), D/Sgt Cyber Investigator - Merseyside Police.

10:15 AM – 10:48 AM

Discussion:

An overview of the team's work was provided, emphasizing the importance of cybersecurity in keeping individuals and organizations safe. It was noted that while basic security measures, such as locking doors at night, are commonly understood, many are unaware of the broader efforts made to protect against digital threats.

Key Points Discussed:

Prepare:
It was highlighted that the team assists organizations and individuals in preparing for compliance with cybersecurity laws, ensuring that legal procedures are correctly followed.

Prevent:
The discussion focused on preventing crime, particularly by supporting neurodivergent individuals. It was explained that the team helps guide these individuals toward fulfilling careers in cybersecurity, such as penetration testing, where salaries start at £60,000 and can go up to £100,000.

Protect:
The team's work in raising awareness about cybercrime was discussed, including collaborations with businesses, charities, and other organizations to share best practices and reduce risk.

Pursue:
It was noted that the team actively pursues cybercriminals, involving arrests, court hearings, and intelligence sharing with international partners, including Russia and Japan.

Cyber Threat Landscape:

The current cyber threat environment was discussed, with approximately half of businesses and a third of charities having experienced some form of cyber attack. The "CIA Triad" – Confidentiality, Integrity, Availability – was reviewed, explaining the impacts of ransomware on personal and professional data.

Types of Threat Actors:
Different cyber threat actors were discussed, including:

- Advanced Persistent Threats (APTs): Stealthy actors that gain unauthorized access to networks.
- Cybercriminals: Individuals primarily motivated by financial gain.
- Hacktivists: Actors driven by ideological motivations.
- Insider Threats: Disgruntled employees or individuals targeting organizations for personal reasons.

Social Engineering:
Various forms of social engineering were explained, including:

- Authority: Exploiting hierarchical structures to manipulate employees into transferring money.
- Urgency: Creating false emergencies, such as ransom demands, to pressure individuals into hasty actions.
- Emotion and Scarcity: Leveraging emotions or a fear of missing out on opportunities to manipulate targets.

Cybercrime Cases and Trends:

DG discussed recent cybercrime cases, including the sentencing of an 18-year-old hacker, Connor Turner, for stealing £66,000. It was noted that phishing attacks have increased, with AI making these scams more sophisticated and harder to detect.

Phishing Threats

It was noted that as of August 2024, 34 million phishing scams had been reported, resulting in 193,000 scams being removed across 352,679 URLs.

Examples of phishing were shown, including very realistic-looking scams such as PayPal emails and fraudulent QR codes. Phishing attacks were explained as generally untargeted and random, designed to catch someone off guard. It was mentioned that AI is now being used by hackers to script phishing emails, making them more difficult to detect. Attendees were reminded to be cautious of URLs, as people can easily spoof calls or emails.

It was also stressed that hyperlinks from unknown sources should **never** be clicked. Attendees were advised to check for unexpected requests with a sense of urgency and look out for poor design and quality in emails (e.g., how they address you, the language used).

Spear Phishing

Spear phishing was discussed as a more advanced form of phishing. These attacks utilize more convincing messages to appear legitimate.

Research of organizations, email spoofing, and the registration of similar domains (e.g., admin@pay-pal.com) are common methods used to trick targets.

Types of Phishing

Different types of phishing were outlined, including spear phishing, smishing (SMS phishing), vishing (voice phishing), and quishing (fraudulent QR codes).

It was reiterated that phishing attacks are not targeted and are random in nature.

AI was mentioned again, with the added note that it makes it more difficult to identify phishing scams due to changes in URLs and spoofing tactics.

The same advice was repeated: **never** click a hyperlink and always check if the request is unexpected and urgent.

Malware and Ransomware

Malware, such as Trojans, was discussed, particularly **Remote Access Trojans (RATs)**, which allow hackers to take control of devices remotely.

Ransomware was mentioned, noting that once hackers gain access to a device, they can encrypt all the data and demand a ransom in exchange for decryption, often directing victims to the dark web.

WannaCry from 2017 was cited as an example, with payments typically demanded in Bitcoin.

Public Wi-Fi Risks

Attendees were warned about the risks of using public Wi-Fi, especially through "man-in-the-middle" attacks, where hackers mirror legitimate networks (e.g., Costa Coffee) to intercept data.

A video was shown to illustrate the dangers of using banking apps on public Wi-Fi.

The use of a VPN was recommended, as it encrypts data between the user's device and the VPN server, making it harder for Internet Service Providers (ISPs) and web services to see personal traffic.

Digital Footprint and Cyber Hygiene

The importance of maintaining good cyber hygiene was discussed. Passwords were emphasized as the first line of defense, with the **National Cyber Security Centre (NCSC)** recommending the use of three random words.

Common attack methods like **dictionary attacks**, **rainbow tables**, and **brute force attacks** were explained.

Password managers were recommended to generate and securely store passwords, with examples including **NordPass**, **1Password**, and **Dashlane**. Attendees were referred to

www.passwordmonster.com, which aims for passwords to have a minimum strength lasting 25 years.

Multi-Factor Authentication (MFA) was highlighted as a necessary measure, requiring something you know (e.g., a password) and something you have (e.g., a phone) to access an account.

Software Updates

The importance of regular software updates was reiterated, with a focus on operating systems, web browsers, extensions, and third-party apps to ensure all security patches are up to date.

Detective Sergeant Danny Gavin
0151 777 4868
Cyber.dependent.crime.unit@merserysid.police.uk
5788@merseyside.police.uk

---

3. Digital Care Hub, Cyber Isn't So Spooky! - Daniel O'Shaughnessy(DS), Head of Programme Delivery

10:48 AM – 11:15 AM

A sector-led consortium, created by and for social care providers, was introduced. The focus is on improving security and care through shared knowledge and free support.

Future of Secure Information Sharing:

Emphasis was placed on securely sharing information, particularly regarding rostering systems, care management systems, eMAR, video calls for staff, families, and GPs, as well as NHSmail and proxy access to NHS systems.

Government Funding:

£150 million in government funding is available for integrated care, supporting the transition from paper to digital systems. More information can be found on the digitising website.

Support Resources:

- LSCP (Local Support Care Partnership) was recommended as the first point of contact for any queries.
- Templates and resources are available on digitalcarehub.co.uk to assist with digital transformation.
- The support offered covers staff and workforce management, IT and software suppliers, and document retention and disposal.

E-Learning Modules:

A free e-learning course covering four modules was introduced:

- Data Protection Rights and Responsibilities
- Keeping Data Safe
- Threats to Data Security
- Data Breaches

Each module takes 20 minutes and provides a certificate upon completion, which can be tracked through a learning management system.

Cyber Incident Checklist:

A checklist for identifying and responding to cyber-attacks was presented, including guidance for managers and steps to contact Action Fraud. It was emphasized that cyber-attacks should be reported as soon as detected to minimize delays in reporting. The ICO must be informed within 72 hours of a breach.

Local Support and Guidance:

Free tailored support is available from 28 local support groups, with 1-to-1 sessions online or in person across England.

Staying Connected:

The Digital Care Hub website and newsletter provide regular updates, webinars, and opportunities to join special interest groups, with an invitation to share case studies for future learning.

11:15 AM – 11:30 AM

Comfort Break | | Tea/coffee and biscuits provided

---

4. Hartland House Case Study: Nobi Smart Lamps - Leanne Scrogham(LS), Registered Manager - Hartland House.

11:30 AM – 11:55 AM

LS's experience in the health and social care sector was outlined. LS worked for four years as a domiciliary care worker and later transitioned to manage a 30-bed care home under the Abbeyfield umbrella in the Lake District during the COVID-19 pandemic.

It was noted that Nobi, founded in Belgium in 2018, is a small company with six offices across Belgium, Austria, the Netherlands, the UK (North Lakes District), and the US (Texas). Nobi's smart lamps are distributed across 21 countries, including Belgium, the Netherlands,

Germany, and the US. The company employs 50 people and is considered a trailblazer in fall prevention technology.

Hartland House was provided with 8 Nobi Smart Lights free of charge for a trial period. The founder's inspiration came from his grandmother's experience with frequent falls and Hartland House was noted as the first UK care home to implement this system.

Fall Management in Health and Social Care:

A variety of fall management methods currently in use were discussed, including:

- Mobility aids
- Night checks (typically every 2 hours)
- Pressure mats, which were described as more of a hazard than a solution
- Acoustic monitoring, smartwatches, nurse call systems, and CCTV

It was highlighted that 80% of individuals cannot call for help after a fall, and only 20% can use traditional nurse call systems.

Nobi Smart Light AI Features:

The Nobi Smart Light system was introduced as a solution to prevent and manage falls more effectively. Key features include:

- Fall prevention, with the ability to prevent 4 out of 5 falls
- Automatic lighting, including night lights
- Fall risk alerts and fall detection, with response times reduced to 4 minutes
- Fall analysis and elimination of long lie falls
- Peace of mind for caregivers and residents due to the system's 100% accuracy
- Smart care capabilities, such as live room monitoring, night reports, and fall analysis reports

It was noted that 64% of falls are often hidden, and Nobi's camera system provides a detailed report of the falls.

Impact of Nobi on Fall Reduction:

LS reported a significant reduction in falls after implementing the Nobi system. Over three months, there was an 84% reduction in falls. It was observed that caregiver response time was reduced from 57 minutes without Nobi to 2.5 minutes with Nobi. She emphasized the benefits of having a Nobi light in every room, though it was mentioned that the system is expensive.

Challenges and Implementation:

It was noted that ICB had commissioned 500 beds across 50 homes to implement the Nobi system. CQC attended the launch of Nobi and raised concerns regarding safeguarding or consent issues if the system is not used correctly.

Case Study:

LS shared a real-life example involving a couple where the wife experienced a fall, and her husband was initially believed to have caused it. However, the Nobi system proved that her husband was not involved, and the fall was due to her dementia.

Q&A Session:

Questions were raised about the placement of Nobi lights in communal areas, corridors, and bathrooms. LS expressed willingness to support anyone interested in using the Nobi system, underscoring her passion for the product.

---

5. AI Use in Social Care – Daniel O'Shaughnessy(DS), Head of Programme Delivery

11:55 AM – 12:10 PM

An overview of the current landscape in social care was provided, focusing on recruitment, retention, and capacity to meet the needs of future communities and workforce trends. The use of AI in these areas was discussed, particularly given the regulatory vacuum in this space.

Oxford Statement on Responsible AI Use in Adult Social Care (ASC):

It was noted that the Oxford Statement outlines principles for the responsible use of AI in adult social care, yet challenges remain in implementation due to the lack of clear guidance.

Current Uses of AI:

Examples of AI use in social care were provided, including:

- ChatGPT used to generate letters for commissioners and to create templates for care plans, such as those for individuals with dementia.
- Concerns were raised about exposing sensitive information to AI systems, with questions about where this data is stored and how it is used.

AI Working Groups:

DS informed the group that DCH contacts who are using AI were invited to form working groups to help decide when and how AI should be used in social care settings. The first project in this space will be shaped by the input gathered during this meeting.

AI applications in HR were discussed, including:

- Using ChatGPT to assist with writing application forms, policies, and procedures.
- A charity was noted to be using AI to help manage overhead costs.

Care plans can be developed with AI, provided that ethical and safety concerns are addressed. However, DS emphasized the current lack of ethical guidance in this area, quoting a representative from Age Concern who highlighted this as a critical gap. It was also mentioned the potential use of location mapping through AI as part of future developments in social care.

It was also explained that current guidance on AI use in social care is still in a working model stage, with confusion around the distinction between AI and algorithms. Attendees were prompted to consider the risks involved with AI, especially regarding data privacy and the potential exposure of sensitive information.

AI for Creative Thinking:

AI's ability to stimulate creative thinking was discussed, particularly for businesses that may struggle with innovation. It was suggested that AI could be used to generate "what-if" scenarios. It was also stressed that personal data should not be shared with AI systems, as there is still uncertainty about where such data is stored and how it is used. DS encouraged participants to stay in touch, ask questions, and remain updated on developments. Contact details for further guidance were provided: Anna.Manetta-Stark@nationalcareforum.org.uk.

---

6. The Latest Trends in Technology in Care and How to Stay Ahead of Them - James Barber, Chief Executive – Jamescape.

12:10 PM – 12:35 PM

The latest technology trends in the care sector was discussed, highlighting his work in developing a SaaS platform aimed at addressing homelessness through data.

Email Security and DMARC Requirements:

It was noted that Google and Yahoo now require DMARC for all emails and organizations, which ensures the authenticity of the emails being sent. Bulk email sending practices were discussed, with a focus on the impact of spam. It was shared that 45.6% of emails are spam, and even genuine emails flagged as spam can harm a domain's reputation. Key recommendations included:

- Setting up DMARC, DKIM, and SPF records to secure emails.
- Avoiding large attachments and using secure (https:) links in emails.
- Ensuring an unsubscribe link is included in bulk emails to reduce spam reports.

The European Accessibility Act (June 2025):

James highlighted the upcoming European Accessibility Act, which will enforce accessibility standards across various systems such as computers, phones, TVs, and ATMs. Key accessibility considerations include:

- Alt text for images and ensuring screen readers can access content.
- Colour contrast and visible keyboard focus for visually impaired users.
- Fully captioned videos, with a note that AI auto-captions are not yet reliable enough.

Password Security and Authentication Trends:

Password security statistics were shared, revealing that:

- 65% of people believe passwords should be written down.
- 77% think changing passwords regularly increases security, though this is not always effective.

The importance of using corporate password managers was emphasized. When employees leave an organization, their access can be revoked through such systems, preventing potential security threats. The group was referred to a list of recommended password management software on TechRadar.

Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) were discussed, with solutions like Twilio Authy and Google's physical authentication keys recommended to enhance security.

The number one security risk for organizations was identified as human error. James emphasized the importance of training and educating staff to prevent cyber incidents. Dial 159 was introduced as a UK-wide pilot initiative to help prevent scams. It allows potential fraud victims to be automatically connected to their bank's fraud prevention service by dialling the number.

A demonstration of identity verification on LinkedIn was referenced, with an example video showing how a single person could appear as different individuals. The group was advised to be cautious and use resources like the Think Before You Link app for verification.

Cyber Incident Response Framework:

The four R's of cyber incident response were shared:

- Respond: Immediate actions taken when a threat is identified.
- Retrospective: Analyzing how the threat was handled and identifying areas for improvement.
- Recover: Steps to return the organization to normal operations or a more secure state.

Closing Remarks:

James concluded by stressing the need for organizations to stay ahead of technology trends, particularly in cybersecurity. He urged attendees to visit Jamescape.net for further insights.

---

8. LSCP updates and Mentimeter Exercise – Ann Garvey(AG)/Mohamed Jaishan(MJ)

12:35 PM – 12:46 PM

AG offered the free support LSCP provides including;

- Cyber Security Awareness and Data Protection training to staff

- DSPT support
- Data security and protection audits which would focus on the data and digital aspects of the business continuity plan.

Lastly, MJ began a mentimeter exercise on the feedback and future of the network.
