# Understanding New Technology Risks

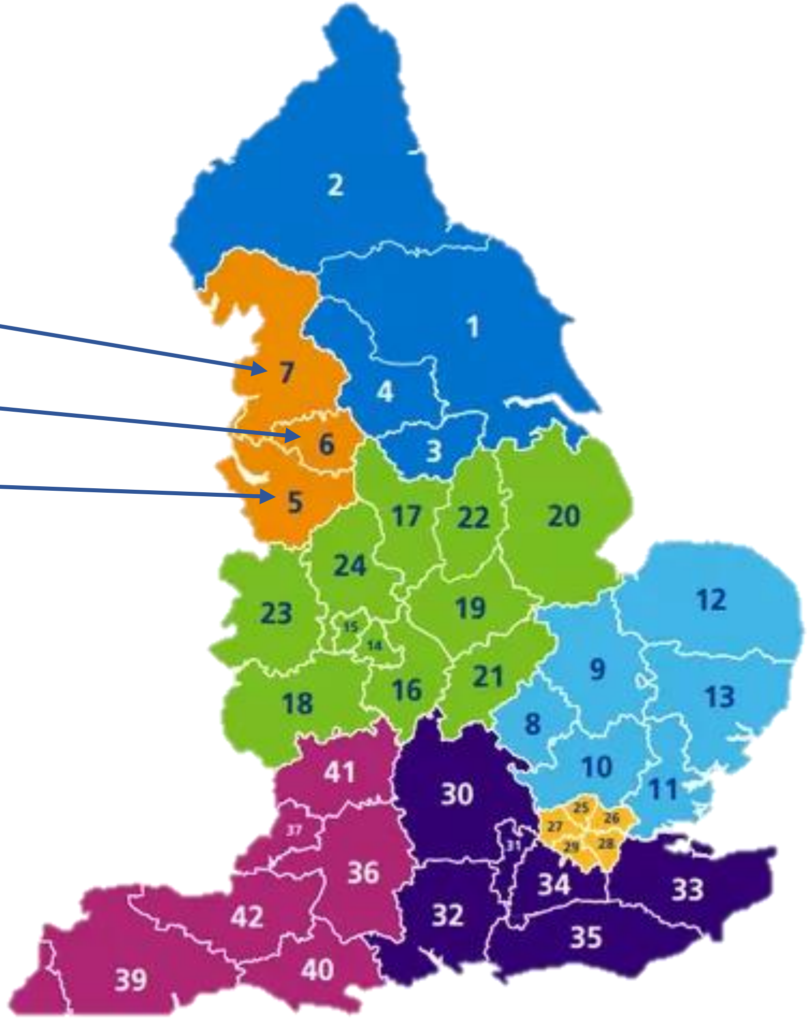
HFMA Audit Conference – 21st March 2024

Paula Fagan and Catherine Watts - MIAA

# Agenda

- Introduction to MIAA Digital Risk Assurance
- Why it Matters
- New Technology in the NHS
- Associated Risks & Supply Chain
- Vulnerabilities and Incidents
- Approaches to Managing Threats
- Key role of the Board & Audit Committee
- Future Skills & Training for Boards and Workforce
- Any Questions
- Key Publications & Guidance

# MIAA & Digital Risk Assurance



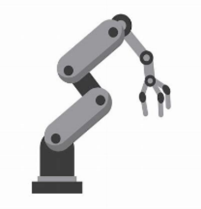
Lancashire & South Cumbria ICB

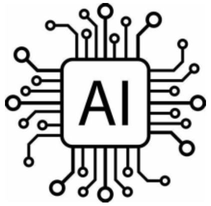
Greater Manchester ICB

Cheshire & Merseyside ICB

- Established 1990
- Provide services to over 70 organisations
- Assurance, Solutions & Corporate Services
- Over 130 staff
- Experienced and skilled team of certified information security professionals
- Over 60 Associates & Partners providing specialist services
- Based in Liverpool, Darwin, Chester & Salford
- One of the largest providers of audit & consultancy services to the NHS, public sector, third sector, charities etc.

# Technology & Risk – why it matters?





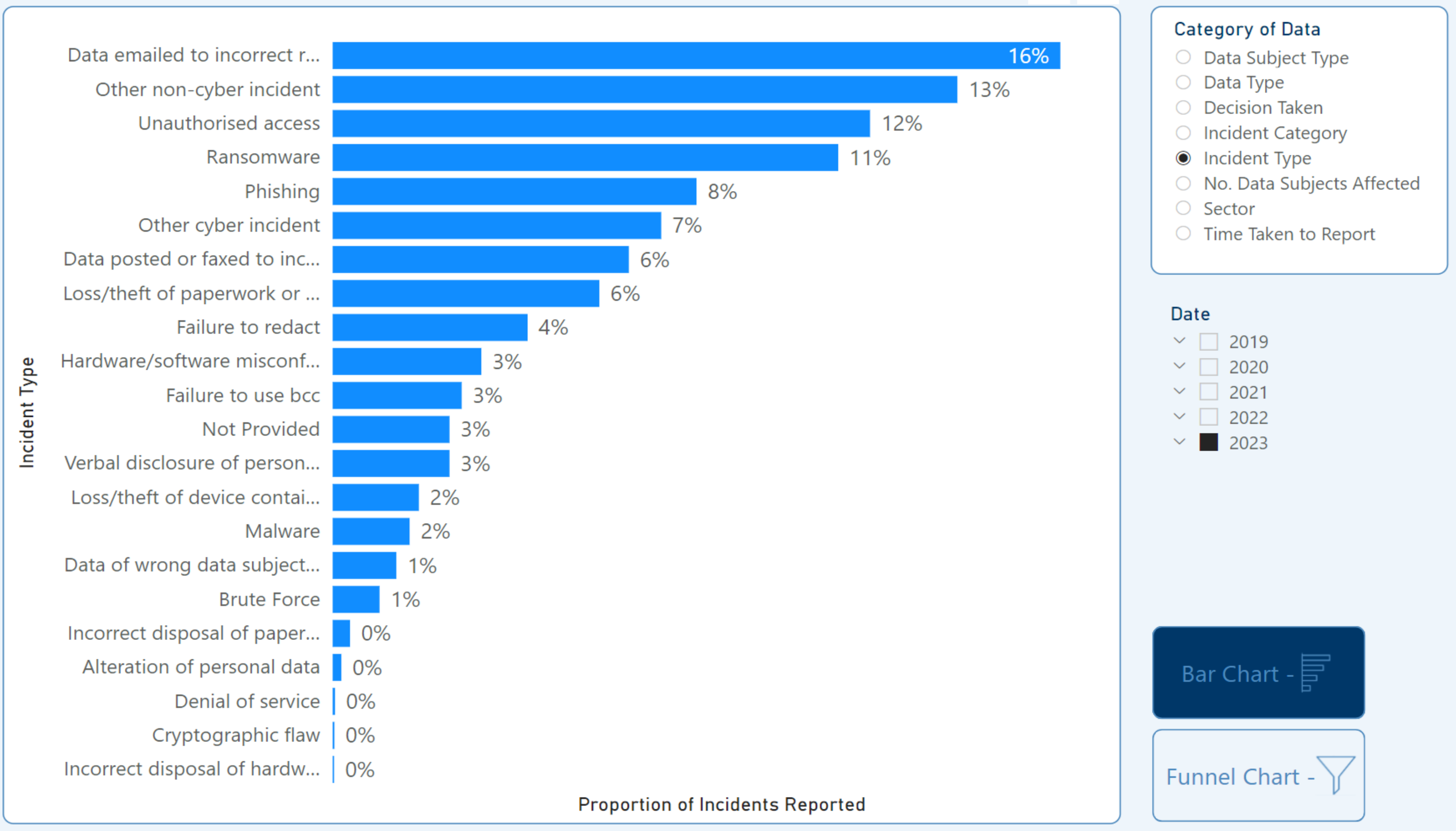
- Patient Care
- Data custodians for patients and staff
- Reputation and reputational damage
- Cyber security strategy can exploit technology, drive an agenda and deliver value
- Supports transformation & change
- Technology is a core function of the organisation
- Key service dependencies on technology

- Cyber security central to operational resilience
- Board understanding to ensure operation resilience against risk and impact of cyber-attacks on business requirements
- Certification pre-requisite for cyber insurance
- Top motivation is financial gain
- Monetary costs incurred as a result of breaches – ICO

# ICO Incidents and Trends (1st July to 31st September 2023)

- 2,715 incidents reported to the ICO – increase of 17% on previous year
- 75% non-cyber related
- 25% cyber related
- Data emailed / sent to wrong recipient the most common incident reported
- Health was the most common sector for incidents, representing 19%
- 49% involved personal data of fewer than 10 people
- 59% of incidents reported within 72 hours of discovery
- Factors influencing further investigation include:
    - Number of data subjects affected, 12% of incidents affecting more than 100,000 data subjects result in an investigation
    - Time taken to report
    - Type of data

# ICO Incidents – proportion of incidents reported


Incident Type
Data emailed to incorrect r... 16%
Other non-cyber incident 13%
Unauthorised access 12%
Ransomware 11%
Phishing 8%
Other cyber incident 7%
Data posted or faxed to inc... 6%
Loss/theft of paperwork or ... 6%
Failure to redact 4%
Hardware/software misconf... 3%
Failure to use bcc 3%
Not Provided 3%
Verbal disclosure of person... 3%
Loss/theft of device contai... 2%
Malware 2%
Data of wrong data subject... 1%
Brute Force 1%
Incorrect disposal of paper... 0%
Alteration of personal data 0%
Denial of service 0%
Cryptographic flaw 0%
Incorrect disposal of hardw... 0%
Proportion of Incidents Reported
Bar Chart -
Funnel Chart -

Category of Data

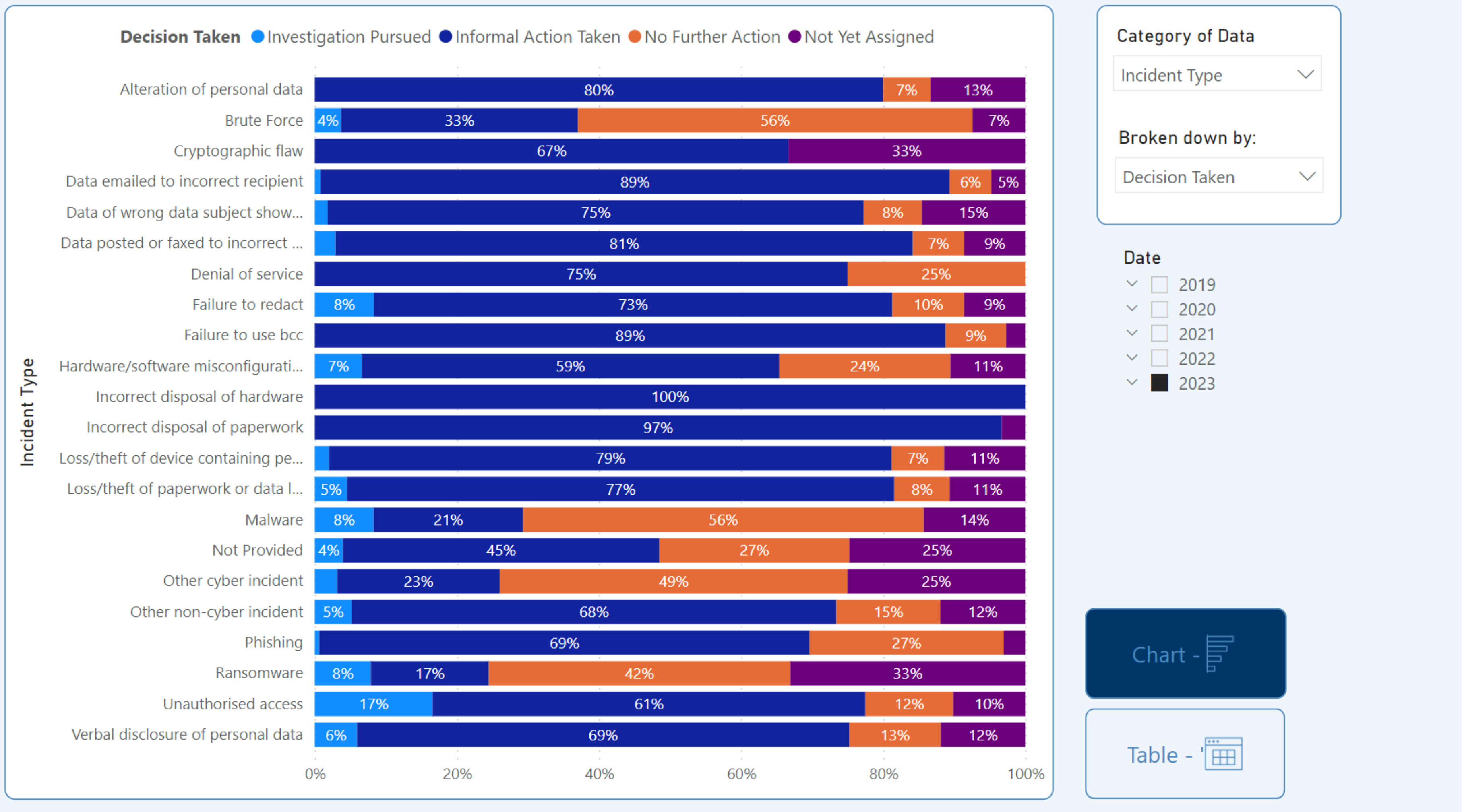
- ○ Data Subject Type
- ○ Data Type
- ○ Decision Taken
- ○ Incident Category
- ● Incident Type
- ○ No. Data Subjects Affected
- ○ Sector
- ○ Time Taken to Report

Date

- □ 2019
- □ 2020
- □ 2021
- □ 2022
- ■ 2023

[Data security incident trends | ICO]

# ICO Incidents – decision taken


Decision Taken ● Investigation Pursued ● Informal Action Taken ● No Further Action ● Not Yet Assigned
Incident Type
Alteration of personal data 80% 7% 13%
Brute Force 4% 33% 56% 7%
Cryptographic flaw 67% 33%
Data emailed to incorrect recipient 89% 6% 5%
Data of wrong data subject show... 75% 8% 15%
Data posted or faxed to incorrect ... 81% 7% 9%
Denial of service 75% 25%
Failure to redact 8% 73% 10% 9%
Failure to use bcc 89% 9%
Hardware/software misconfigurati... 7% 59% 24% 11%
Incorrect disposal of hardware 100%
Incorrect disposal of paperwork 97%
Loss/theft of device containing pe... 79% 7% 11%
Loss/theft of paperwork or data l... 5% 77% 8% 11%
Malware 8% 21% 56% 14%
Not Provided 4% 45% 27% 25%
Other cyber incident 23% 49% 25%
Other non-cyber incident 5% 68% 15% 12%
Phishing 69% 27%
Ransomware 8% 17% 42% 33%
Unauthorised access 17% 61% 12% 10%
Verbal disclosure of personal data 6% 69% 13% 12%
0% 20% 40% 60% 80% 100%
Chart -
Table -

Category of Data
Incident Type

Broken down by:
Decision Taken

Date
□ 2019
□ 2020
□ 2021
□ 2022
■ 2023

[Data security incident trends | ICO]

# ICO Incidents – Action Taken (1 monetary penalty)

***NHS Foundation Trust, 30 Jun 22, Monetary penalties, for using Outlook to send bulk emails to 1,781 Gender Identity Clinic service users.***

£78,400

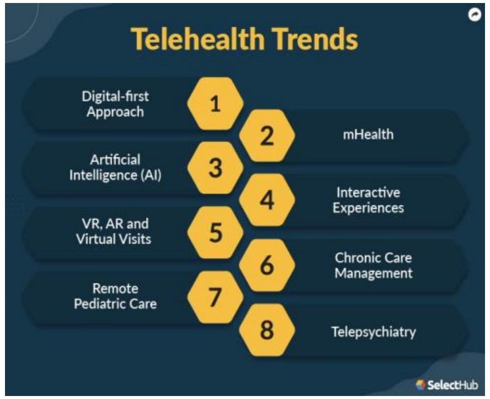
[Enforcement action | ICO]

# ICO Incidents – Action Taken (12 Health reprimands)

| | |
|---|---|
| 20 Dec 23 | Failure to ensure staff fully training and prepared to deal with particularly sensitive correspondence |
| 23 Nov 23 | Unauthorised individual entered ward and accessed personal information of 14 patients |
| 30 Oct 23 | Failure to ensure adequate processes in place when processing special category data, resulted in refer |
| 31 Jul 23 | Sharing of personal data of patients via unauthorised means and secondly, a disclosure of personal data |
| 19 Jul 23 | Disclosure of special category data due to an email sent to 15 individuals using (CC) not (BCC) |
| 25 Apr 23 | Certain infringements of the UK GDPR |
| 9 Mar 23 | Email to 37 people accessing HIV services using (CC) instead of (BCC) |
| 7 Mar 23 | Number of records became inaccessible / some permanently lost |
| 3 Mar 23 | Inadvertently released untested development code into a live system for matching patients |
| 10 Nov 22 | Scans saved onto USB sticks became inaccessible |
| 7 Apr 22 | Incorrect test results passed to Public Health resulting in individuals being erroneously contacted |
| 24 Feb 22 | Breach of UK GDPR – processing personal data, including special category data unfairly |

Enforcement action | ICO

# Introduction to new technology within the NHS

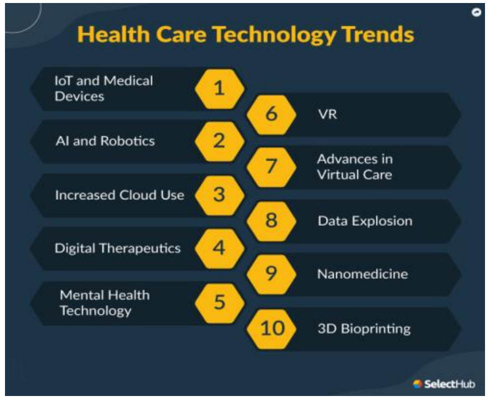


## Telehealth Trends

1. Digital-first Approach
2. mHealth
3. Artificial Intelligence (AI)
4. Interactive Experiences
5. VR, AR and Virtual Visits
6. Chronic Care Management
7. Remote Pediatric Care
8. Telepsychiatry

SelectHub

- Virtual wards and assistance
- Telemedicine
- Mobile healthcare
- Internet of "wearable" medical devices
- Diagnostic 3D and imaging technology
- 3D printing / nanomedicine
- Big Data
- AI algorithms to tackle patient flows
- Decision support
- Generative AI to customise journeys
- Digital twins / virtual models
- Immersive technology / VR
- Enhanced regulatory compliance requirements
- Integrated vendor partnerships
- Applications – NHS App / EPR
- Cloud



## Health Care Technology Trends

1. IoT and Medical Devices
2. AI and Robotics
3. Increased Cloud Use
4. Digital Therapeutics
5. Mental Health Technology
6. VR
7. Advances in Virtual Care
8. Data Explosion
9. Nanomedicine
10. 3D Bioprinting

SelectHub

# Spring Budget UK 2024 - £3.4 billion to invest in NHS digital transformations

NHS App to be the single front door through which patients can access NHS services / manage their care

Digitally-enabled prevention / early intervention services

Delivering a radically improved online experience for patients – open / online

Pilots to test Artificial Intelligence (AI) to automate back-office functions

Provide NHS staff with digital passports / access to a new NHS Staff App

Acceleration of the Federated Data Platform (FDP) to bring together operational & ICS data currently stored on separate systems to every trust in the country by the end of 2026-27

Upgrading IT systems, scaling up existing use of AI & ensuring all NHS staff are equipped with modern computing technology

Ensuring all NHS Trusts have EPRs by March 2026

Upgrading over 100 MRI scanners with AI

Digitising transfers of care

# Risks from new technology & the supply chain

## Supply Chain Attacks Surge

- Suppliers can pose various risks, for example in terms of third-party access to systems, suppliers storing personal data or IPR, and originating phishing attacks, viruses or other malware.
- Exploiting interconnected networks
- High-profile breaches targeted the supply chains of major corporations
- Highlights the need for robust cybersecurity measures throughout entire ecosystems

## Cloud Security Challenges

- As businesses continue to migrate to cloud-based environments, cyber attackers shifted their focus to exploit vulnerabilities in cloud services
- Misconfigurations, inadequate access controls, and insufficient data encryption practices led to a surge in cloud-based attacks
- The challenge is to enhance cloud security through proper configuration management and comprehensive monitoring

# Risks from new technology and the supply chain

## Ransomware-as-a-Service (RaaS) Dominance

- Lower entry barrier for aspiring criminals, contributing to the proliferation of ransomware incidents

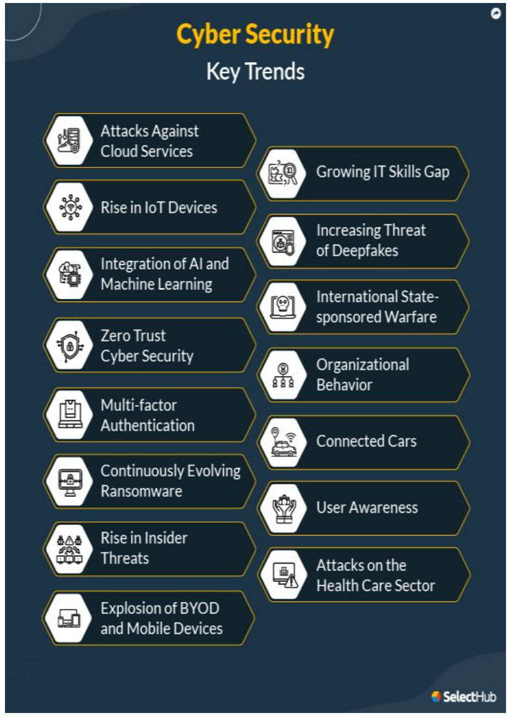
## Zero-Day Exploits and APTs

- Advanced Persistent Threats (APTs) exploiting zero-day vulnerabilities
- targeted high-value assets, utilising undisclosed vulnerabilities to gain unauthorised access
- Need to adopt proactive security measures and rapid patching to mitigate risks

## Artificial Intelligence (AI) / Social Engineering Attacks

- ChatGPT and competitors, targeted Phishing, Deep Fakes, malware injection, etc. User awareness and training should be maintained.

# Global examples of incidents



**Cyber Security**

Key Trends

- Attacks Against Cloud Services
- Rise in IoT Devices
- Integration of AI and Machine Learning
- Zero Trust Cyber Security
- Multi-factor Authentication
- Continuously Evolving Ransomware
- Rise in Insider Threats
- Explosion of BYOD and Mobile Devices
- Growing IT Skills Gap
- Increasing Threat of Deepfakes
- International State-sponsored Warfare
- Organizational Behavior
- Connected Cars
- User Awareness
- Attacks on the Health Care Sector

SelectHub

Aug 2022 - Last Pass a password manager - Hackers accessed archive data held on a third-party cloud.

Nov 2022 - Crypto jacking – mining crypto currency on cloud devices without consent

20 Dec 2022 - The Guardian newspaper suffered a ransomware attack

Aug 2023 - UK electoral commission issued a note - database was breached / 40m people’s data exposed in Oct 2022

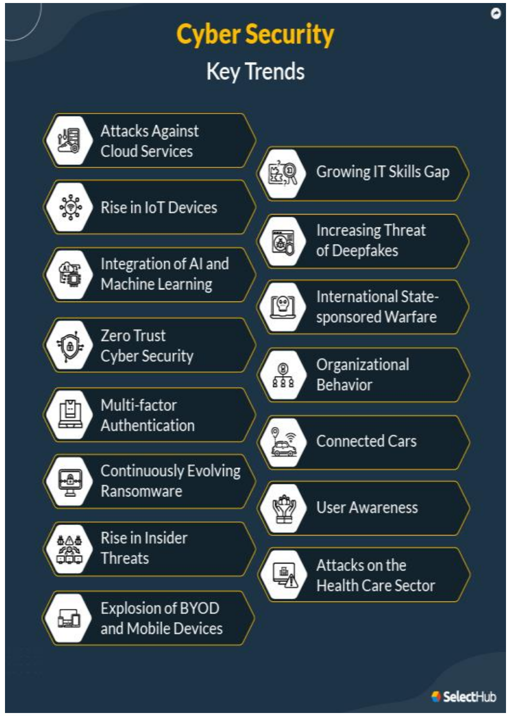
2023 - US casino chain Caesars – database of customers stolen / suffered a ransomware attack

Microsoft storm 0558 – a Chinese hacking group obtained a consumer key. Access was gained to OWA and outlook for 25 organisations. It impacted several US Govt departments

Jan 2023 - Royal Mail / Emotet malware was detected / an affiliate attacker used LockBit Ransomware-as a service for the attack

Jan 23 - MOVEit software used a previously known SQL injection vulnerability to infect web applications.  Victims exceed 2000 organisations / 60 million+ people

# Examples of specific vulnerabilities and incidents



Cyber Security

Key Trends

- Attacks Against Cloud Services
- Rise in IoT Devices
- Integration of AI and Machine Learning
- Zero Trust Cyber Security
- Multi-factor Authentication
- Continuously Evolving Ransomware
- Rise in Insider Threats
- Explosion of BYOD and Mobile Devices
- Growing IT Skills Gap
- Increasing Threat of Deepfakes
- International State-sponsored Warfare
- Organizational Behavior
- Connected Cars
- User Awareness
- Attacks on the Health Care Sector

SelectHub

Feb 23 – vulnerability for Infusion pump monitoring software

Dec 22 - infusion pump – accessible through a serial port / physical access needed. No PII stored in the pump

Nov 22 – smartphone-based software vulnerability for an EKG device. Attacks need to be close by for DOS attackand / or to steal / fake cardiograms

Sep 22 – potential issue with an insulin pump under specific circumatnances

July 22 – zero-day SQL injection authentication bypass of a PACS server

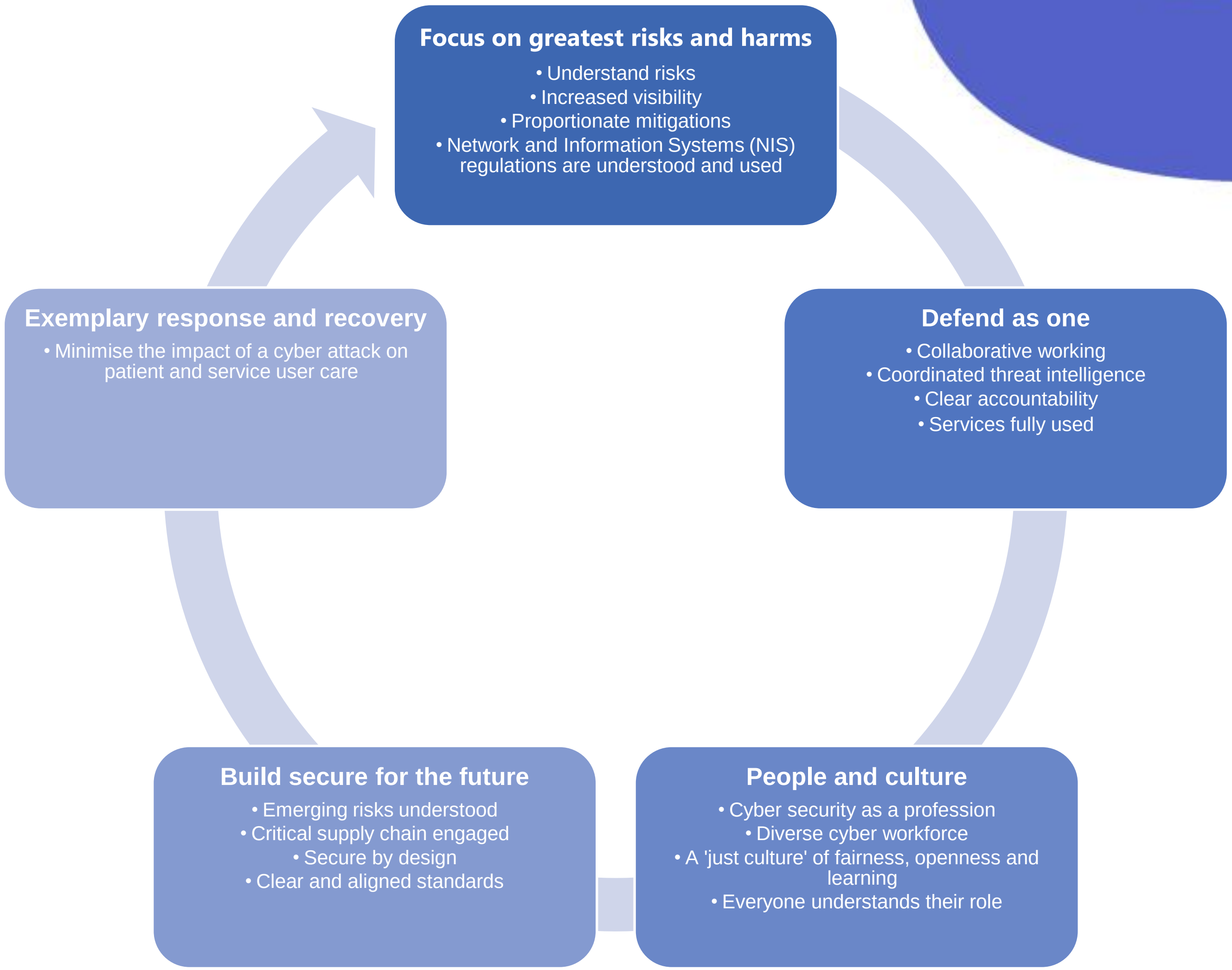
April 22 – 5 zero-day vulnerabilities for a server used to communicate with mobile robots in hospitals – control / access data

May 21 – 2 vulnerabilities of critical severity for medical device products – to allow remote execution / DOS on device

Mar 21 – 6 vulnerabilites on a medical device – escalation of privileges and use of hard-coded credentials possible

# Examples of approaches for managing threats

- Being situationally aware
- Using data / user analytics capabilities
- Baselining assets and effective logging and monitoring
- Effective management of third parties
- Secure by design principles
- Cyber training awareness
- Application allow lists / network segmentation /
- Multi Factor Authentication / access controls
- Guidance, compliance and legislation
- Leadership - role of the board (being informed / checking mitigations and metrics / providing focus)



**Focus on greatest risks and harms**

- Understand risks
- Increased visibility
- Proportionate mitigations
- Network and Information Systems (NIS) regulations are understood and used

**Defend as one**

- Collaborative working
- Coordinated threat intelligence
- Clear accountability
- Services fully used

**People and culture**

- Cyber security as a profession
- Diverse cyber workforce
- A 'just culture' of fairness, openness and learning
- Everyone understands their role

**Build secure for the future**

- Emerging risks understood
- Critical supply chain engaged
- Secure by design
- Clear and aligned standards

**Exemplary response and recovery**

- Minimise the impact of a cyber attack on patient and service user care

# Examples of approaches for managing threats

| Activities to identify cyber security risks in the last 12 months | Businesses | Charities |
|---|---|---|
| Any of the listed activities | 51% | 40% |
| Used specific tools designed for security monitoring | 30% | 19% |
| Risk assessment covering cyber security risks | 29% | 27% |
| Tested staff (e.g. with mock phishing exercises) | 19% | 16% |
| Carried out a cyber security vulnerability audit | 15% | 14% |
| Penetration testing | 11% | 9% |
| Invested in threat intelligence | 9% | 7% |

Cyber security breaches survey 2023 - GOV.UK (www.gov.uk)

# Cyber Hygiene practices for managing threats

| Cyber hygiene practices |
|---|
| Offline encrypted backups and data at rest (confidential data) |
| Awareness and training of healthcare professionals |
| Regular vulnerability scanning |
| Good practices for authentication including remote access |
| Cyber incident response plans / contingency plans (tested) |
| Clear communications channels and planned care for staff |
| Commitment of senior management is key, with NIS2 (CAF) introducing liabilities for top management |

ENISA (European Union Agency for Cyber Security) Threat Landscape: Heath Sector July 2023

# Key Role of the Board and Audit Committee

Framework for managing cyber risk:

- Step 1 – establish organisational context
- Step 2 – Identify decision makers, governance processes and constraints
- Step 3 – define your cyber security risk challenge
- Step 4 – select your approach
- Step 5 – understand risks and how to manage them
- Step 6 – communicate and consult
- Step 7 – implement and assure
- Step 8 – monitor and review

Cyber Security Toolkit for Boards - NCSC

# Key Role of the Board and Audit Committee

- Leadership - role of the board
  - enabling the organisation to focus on key risks / harm
  - measuring cyber security effectively
  - Not experts but providing appropriate challenge
- Support - role of the board
  - ensuring sufficient resourcing
  - proactive engagement

# Future skills & training for Boards and Workforce

- Challenges - HSJ workforce, global shortages
- Training Needs Analysis – Cyber skills for all
- Approaches to training provision
- Support for bespoke / specialist skills and certification
- Support secondments, intern placements, apprenticeships
- Forums and events
- Regular communications and briefings
- Evaluation - role of audit and assurance

# Any Questions ?

# Key publications & useful documents

- Cyber Security Strategy for Health & Adult Social Care to 2030
- Medicines and Medical Devices Act 2021
- The Data Protection Act 2018
- The Cyber Assurance Framework (CAF)
- Framework for conducting annual appraisals of NHS chairs (CAF)
- NHS England: multi-factor authentication (MFA) policy
- UK Spring Budget 2024
- ENISA – Threat Landscape – Healthcare
- ISO standards including ISO 27000 (IT) and ISO 13485 (medical devices)
- NCSC Board toolkit resources
- Briefing notes by MIAA

**Catherine Watts**
Principal Digital Risk Consultant
Tel: 07554 338496
Email: catherine.watts@miaa.nhs.uk

**Paula Fagan**
Head of Technology Risk – Digital Assurance and Solutions
Tel: 07825 592866
Email: paula.fagan@miaa.nhs.uk

miaa