Summer Schools 2023
a digitalhealth event
27–28 July

#DHSS23

Bridging the gap: linking national and local efforts in cybersecurity strategy

Chair: James Hawkins

Chief Digital Information Officer, York and Scarborough Teaching Hospitals NHS Foundation Trust

Mike Fell

Executive Director of National Cyber Security Operations
NHS England

Nick O'Reilly

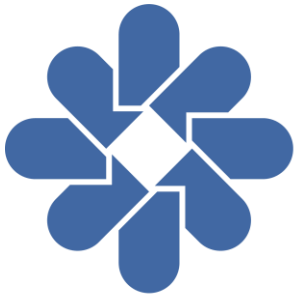
Director of Digital
NHS Birmingham and Solihull ICB

Phil Huggins

National Chief Information and Security Officer for health and social care
NHS England

Andy E

Chief Cyber Security Officer
Birmingham and Solihull ICS



Summer Schools 2023

a digitalhealth event

27–28 July

#DHSS23

Nick O'Reilly & Andy Evans

Director of Digital Chief Cyber Security Officer

Birmingham and Solihull Integrated Care System

Birmingham and Solihull Integrated Care System
Caring about healthier lives

About Birmingham and Solihull ICS

Our ICS supports 1.36 million people living in Birmingham and Solihull.

Our priorities are to:

- Reduce inequalities - improving quality of care by tackling differences in experiences and outcomes for patients
- Integration - work together to join up services and help them work better together
- Protect people from harm – prepare for emergencies and work together on approaches to infection control, immunisation and screening
- Be there for people throughout their life, from birth to end of life care
- Build, develop and retain a great, inclusive workforce
- Contribute to the wider factors of health - such as employment, education and environmental sustainability and recognise our role in growing the local economy

Our Places and our Partnership

The map shows the location of our major secondary care providers across our local health and care system

List of partners

Birmingham City Council

Solihull Metropolitan Borough Council

158 general practices

Birmingham and Solihull Clinical Commissioning Group

Birmingham and Solihull Mental Health NHS Foundation Trust

Birmingham Children's Trust

Birmingham Community Healthcare NHS Foundation Trust

Birmingham Women's and Children's NHS Foundation Trust

The Royal Orthopaedic Hospital NHS Foundation Trust

University Hospitals Birmingham NHS Foundation Trust

West Midlands Ambulance Service University NHS Foundation Trust

Digital Strategy

Strategic Objectives:

1. **Levelling Up -** The disparities of health and care provision between areas are eliminated.

2. **A harmonised system-first approach -** The ICS adopts a system-first approach to provide a care system that allows seamless collaboration across organisations.

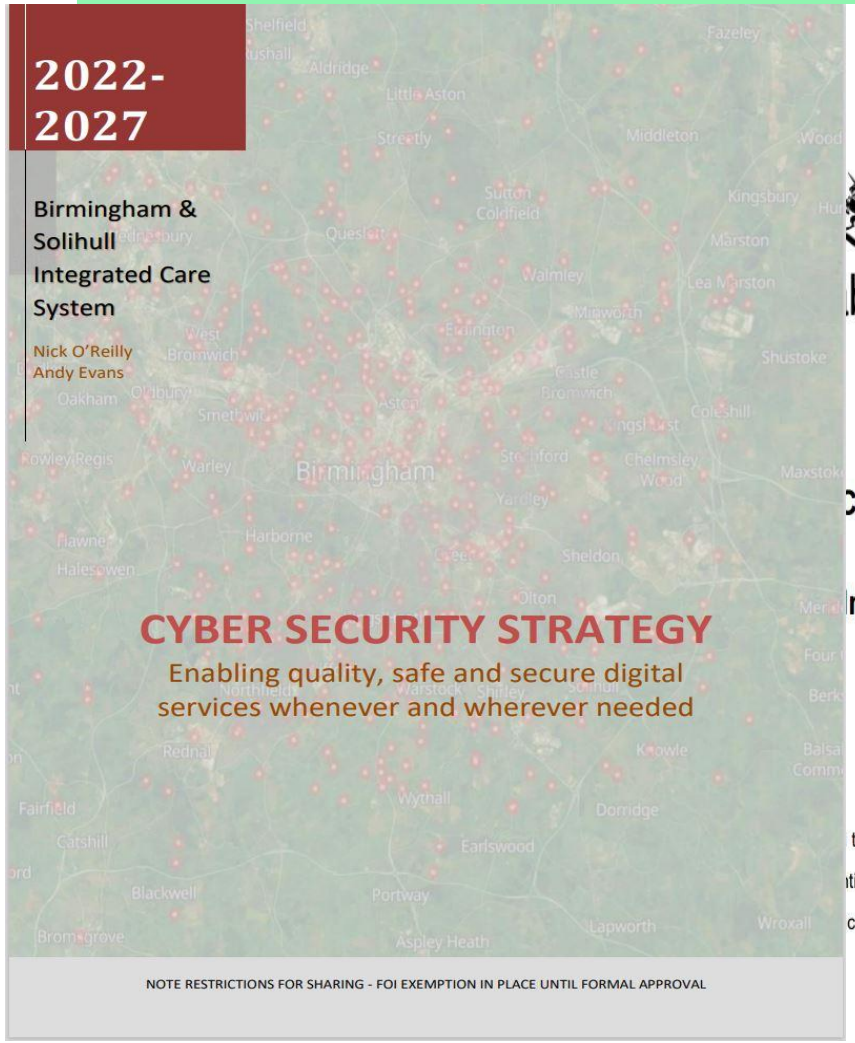
3. **Shared Care Record -** A Shared Care Record is fundamental to delivering cohesive ICS wide care.

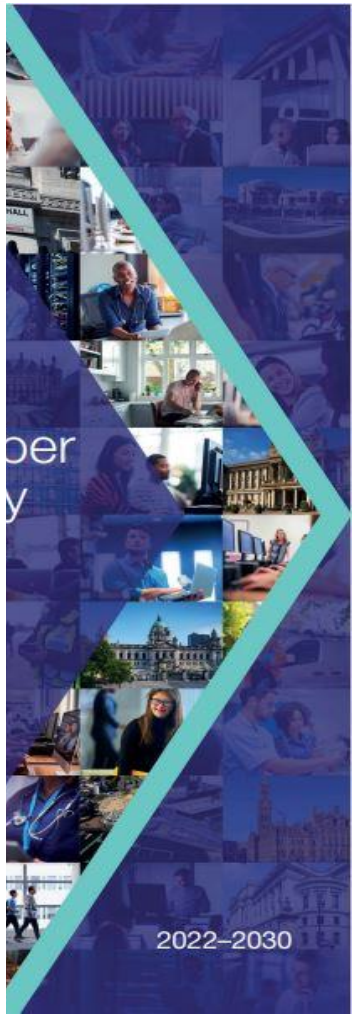
4. **Digital First for Better Care -** Digital solutions should enable an improvement in health outcomes and care quality.

5. **Safe -** A holistic view of Clinical and Cyber safety is culturally embedded in Birmingham and Solihull ICS.

Birmingham and Solihull Integrated Care System
Caring about healthier lives

Bridging the Cyber Security gap: linking national and local Cyber strategies (and others)





The starting point

NHSE's 'What Good Looks Like' framework, shared cyber security problems and opportunities impacting the ICS and its constituent organisations.

WGLL Framework
The 'What Good Looks Like' (WGLL) framework is directed at NHS leader as they work out 'what good looks like' both a **system and** organisational level, defining success measures to accelerate digital and data transformation. WGLL is part of the ICS design framework.
Three Themes:
- Connect
- Transform
- Digitise

WGLL Measures	WGLL Cyber and Information Risk Measure (*Summary*)
Well Led *(Governance)*	ICS Boards regularly review and are invested with development sessions, to be build confidence managing cyber and information security risk, underpinned by effective metrics
Ensure Smart Foundations (*Systems and Teams)*	Ensure systems (*hard/soft)* and networks are supported and secure throughout their life cycle, with all projects and programmes meeting the Technology Code of Practice and cyber secure be design principles.
Safe Practice (*Process, technology and capabilities)*	Comply with agree cyber and data risk frameworks, ensuring process for managing cyber risk (*strategy to operation)* are embedded and reviewed across organisations. Establish ICS wide process for reviewing and responding to relevant safety recommendations and alerts (*incidents).* Ensure adequately resourced cyber security function, roles (*SIRO)* and responsibilities are defined. Embed an ICS system-wide plan for maintaining robust cyber security, including view of central v local capabilities and services provided.
Support People (*People)*	Support staff to attain a basic level of data, digital and cyber security literacy, followed by continuing professional development; (*Human Factor)*

Future state behaviours/attributes

- Risk appetite set by the business and agreed.
- Cultural change leading to business ownership
- Clear accountability defined along with expectations
- Recognising risk to the business from IT Threats

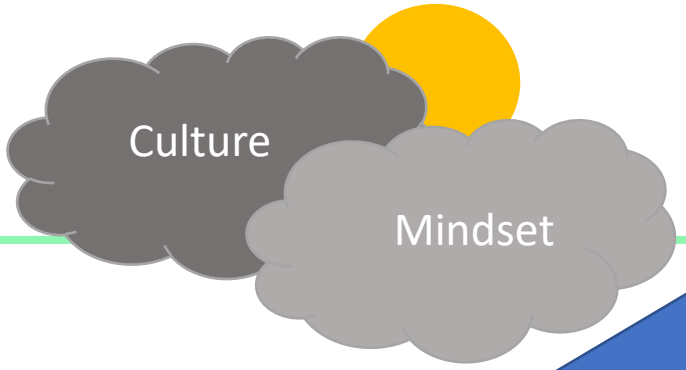
- Implementation and monitoring fundamentals in place enabling mature operational processes
- An inherent secure by design approach to EA, posture and controls
- Visibility and maintenance of technology assets , understanding of their lifecycle vulnerabilities
- Controls delivering corporate policy such as secure by design, understanding assets, component technologies etc.
- Supplier/Vendor assurance throughout the lifecycle
- Defined Cloud migration expectations, plans management and control

- Business owned and relevant metrics and KPIs
- Managed responses to vulnerabilities within defined times with strong supporting processes and systems.
- Strong cooperation between ITOps, cyber and information risk teams: shared functional agenda.
- Agreed standards and frameworks for data and cyber security resiliency and the assurance of compliance to these
- Making best use of service availability and shaping requirements for national cyber service

- Focus on the Human Factor risks and vulnerabilities: motivating and mobilising the human firewall
- Using strong containment and response including automating security.
- Cyber education for general staff across the NHS and requirements for cultural changes.
- Training and development for all Digital Services and ITOps
- Making the NHS a place people WANT to work in cyber

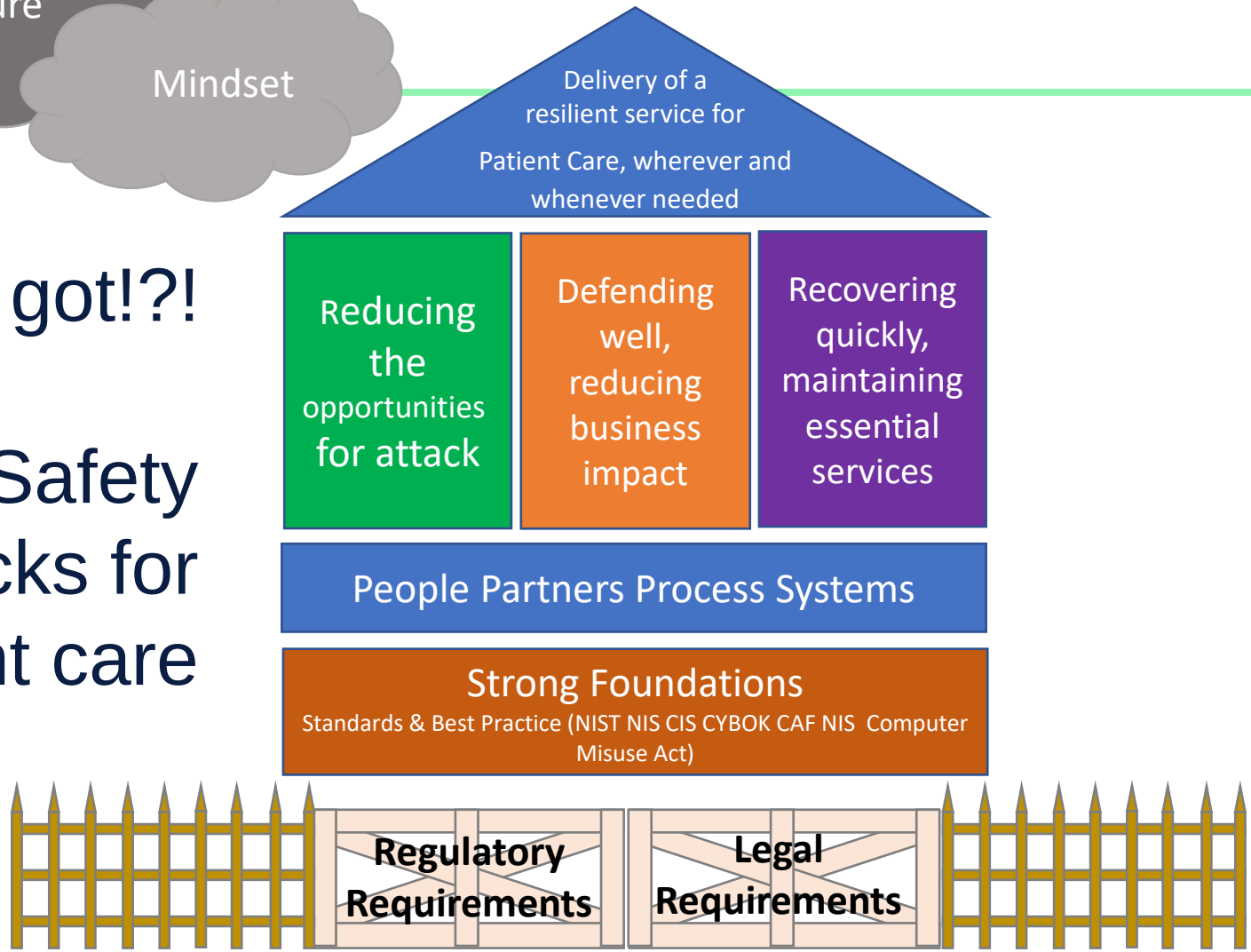
“It’s a TEAM GAME” - Technology is always the *easy* bit – it is the people that make it work

Birmingham and Solihull Integrated Care System
Caring about healthier lives



And this is what we got!?!

Our Health & Safety building blocks for delivering patient care



Birmingham and Solihull Integrated Care System
Caring about healthier lives

How do WE get there?

One step at a time…

We don't need to invent anything

We copy, steal and standardise with pride (and credit)

The best way to do it is already available (Cybok, NIST, NCSC & you)

Collaboration does not mean a single system, service or approach

Working together we will co-operate, co-produce, collaborate and challenge

Of course, it makes sense to work together and share where we can

Birmingham and Solihull Integrated Care System
Caring about healthier lives

Aligning Security with Patient Safety

Key considerations:

Our core business is CARE not IT – IT is the enabler

“Good security metrics should align with business drivers and risks” - (SANS institute)

“Vulnerability leads to Threat Assessment; Threat Assessment informs Business Risk”

Birmingham and Solihull
Integrated Care System
Caring about healthier lives

CAF is at the core of our strategy (and *must* be to yours)

KPIs running “floor to board” is essential

Cyber can be, and should be boring

When your security posture strategy is only for compliance.

Birmingham and Solihull Integrated Care System
Caring about healthier lives

Key Performance Indicators – Aligning Security with Patient Safety

1. Vulnerability – how many of the technical "known in exploit" list of threats do organisations have?
2. How many of the systems have an identified **(information asset) owner**?
3. How many systems of the systems have been assessed?
4. How many systems have incident response/business continuity plans that have been tested?

They are; simple, measurable, impactable and relevant to the need. The impact of collection is negligible

Objective: to monitor and manage ICS Partner threat, risk and readiness for an incident that would impact clinical safety and operational performance

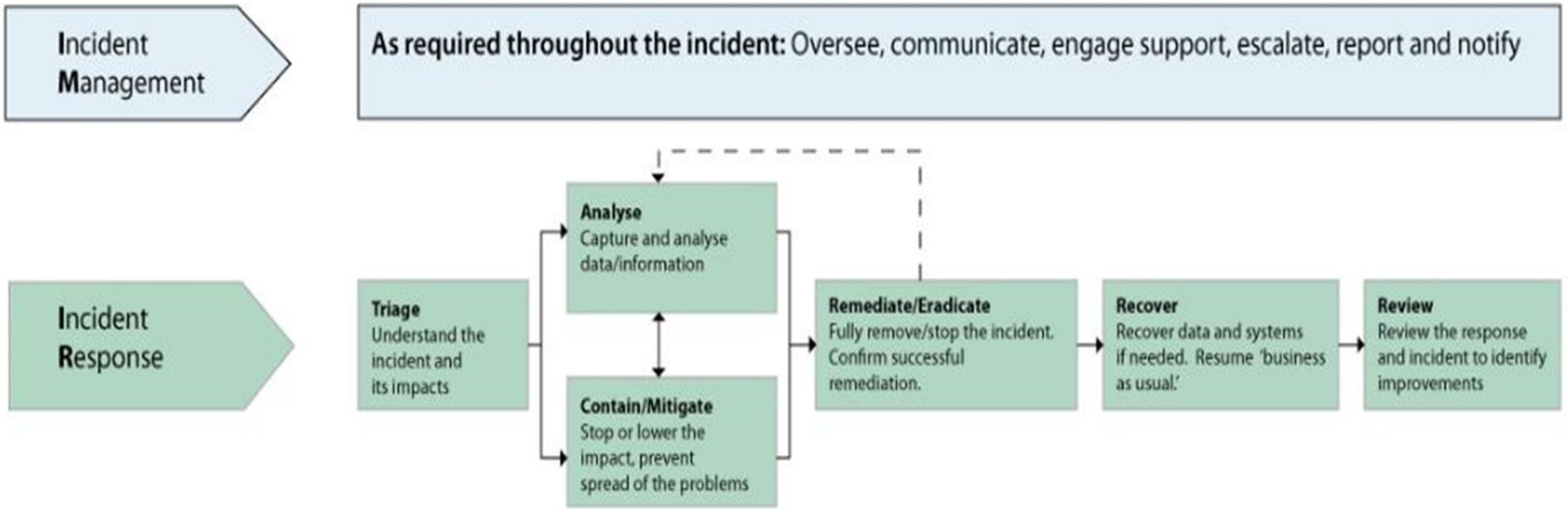
Birmingham and Solihull Integrated Care System
Caring about healthier lives

Quick Wins and Watch Outs

- A BSOL Cyber "FAMILY" – including NHSE
- Developing "Cheerleaders"
- Board development sessions - building trust
- War gaming & exercising – very regularly
- Making ICS wide use of one-off funding
- Asset Management
- True understanding of our external threat surface (and monitoring)
- Recon of all new suppliers and Local Assurance Framework
- Early warning systems
- Basic shared learning and webinars

- Weakest Link - **we only need one of you to be worse**
- What we need – what we don't need approach
- Limited Resources –use wisely
- Clarity in who does what and who doesn't do what (local and national)
- Wary of snake oil cyber systems
- Not more gadgets and toys – people, partners and process
- Shadow IT, there is danger in the shadows

Shared working and common process – Example; Incident Management



Birmingham and Solihull Integrated Care System
Caring about healthier lives

NEVER WASTE A GOOD DISASTER

Cloudflare Radar

Last 4 weeks | Apr 07 2023 17:49 UTC

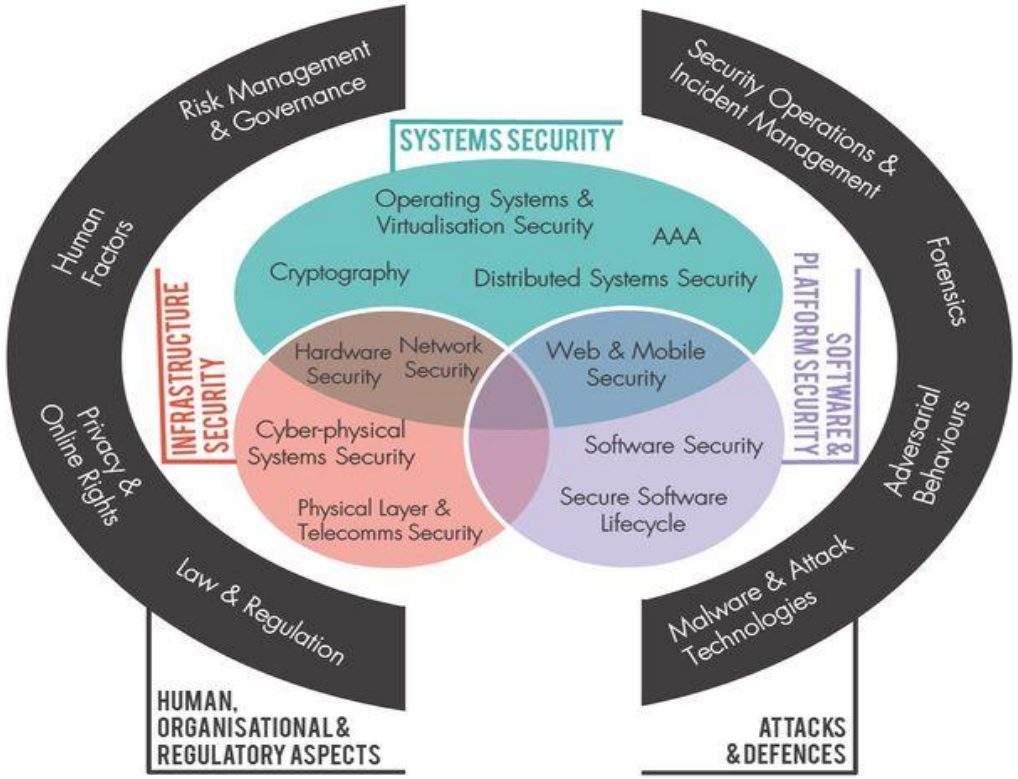
Birmingham and Solihull Integrated Care System
Caring about healthier lives

What do we need

…so we can be successful in delivering the national and local strategies?

1. Resources – in the right places
2. Funding – not just capital (if capital then we need to think about how we best use that)
3. Legacy replacement priority programme linked to risk
4. Who is doing what, who pays for what, what is national v local service/system?
5. Focused Board and senior management, clinician engagement and coaching/mentoring/development
6. Honesty
7. Policy that means something – holding to account

Where do WE want to be? (One for the techies)



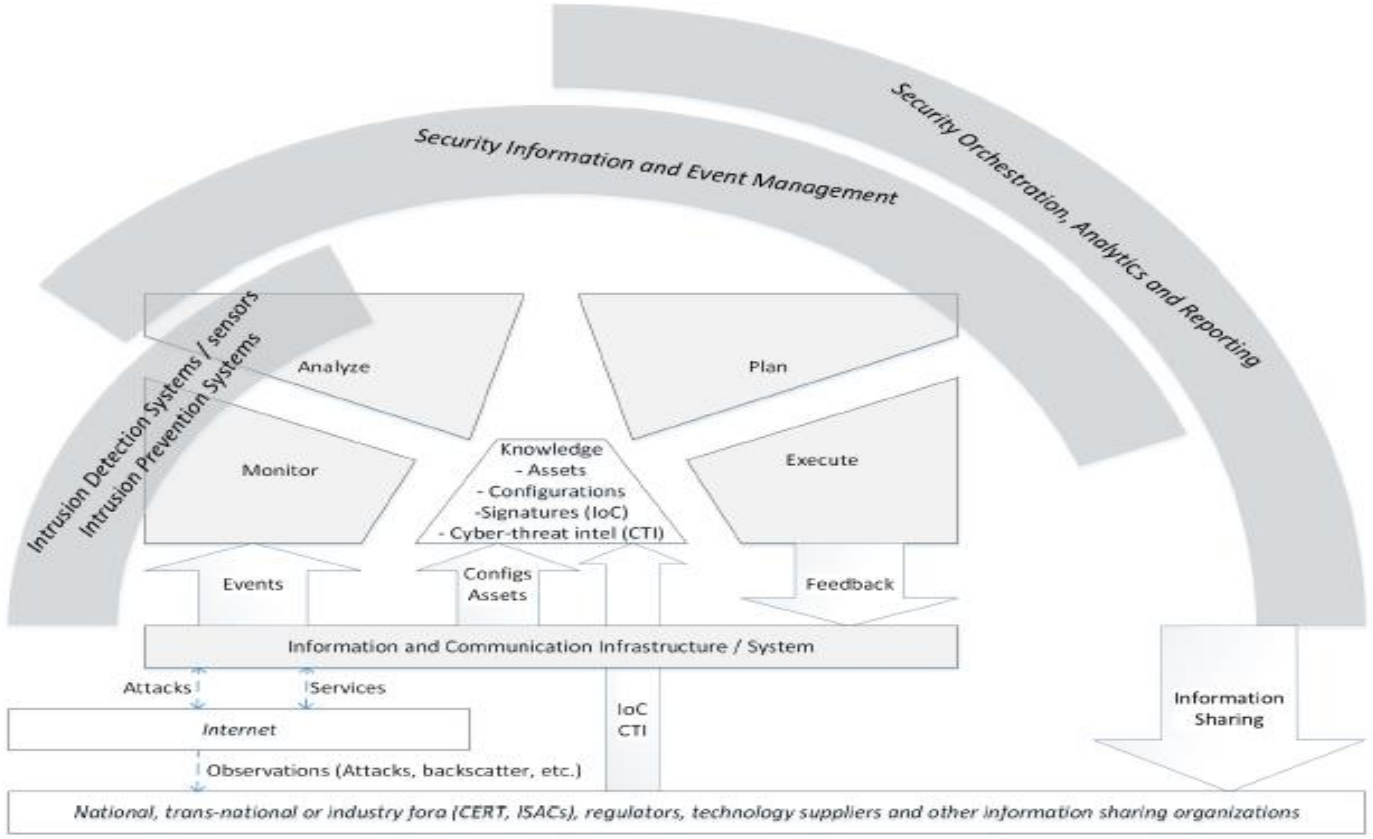


Figure 8.1: MAPE-K Autonomic computing loop instantiated to SOIM

Thank you for listening

Summer Schools 2023
a digitalhealth event
27–28 July

#DHSS23

Bridging the gap: linking national and local efforts in cybersecurity strategy

Chair: James Hawkins

Chief Digital Information Officer, York and Scarborough Teaching Hospitals NHS Foundation Trust

Mike Fell

Executive Director of National Cyber Security Operations
NHS England

Nick O'Reilly

Director of Digital
NHS Birmingham and Solihull ICB

Phil Huggins

National Chief Information and Security Officer for health and social care
NHS England

Andy E

Chief Cyber Security Officer
Birmingham and Solihull ICS