INSIGHTS
BRIEFING
July 2024

DIGITAL ICS

Keeping your integrated care system safer from cyber attacks

Public sector organisations are increasingly under attack from organised groups who are searching for vulnerabilities and opportunities to massively disrupt your services and profit from doing so. The criminals' focus is not just on preventing you from doing your work, but also holding your organisation to ransom for access to data, and in many cases, data theft for profit.

There is no such thing as 'safe', only *safer*. But you can be better prepared to respond when, not if, you face disruption in your integrated care system (ICS) from an attack, where potentially the impact can last for a long time.

Here are five top tips and a series of questions to help ICS leaders ensure they are prepared and able to respond to cyber threats.

1

Understand that every board member and senior leader has a role in keeping your system safer

Every leader, both executive and non-executive, needs to be able to seek and gain assurance on cyber so it's important to educate yourselves.

- As a board, how do you have the conversations to make sure you are as prepared as possible for a cyber attack? For example, does everyone understand what 'patching' means and why it's important? Do you actively talk to peers about what they've learned from being a victim of an attack?
- As a board, how do you ensure that you are seeing and responding to a holistic picture of risk across the system?
- How will you find out what your blind spots are – both your system vulnerabilities and your gaps in understanding and confidence?
- As leaders, are you spending time with the teams who are doing the work? Risk can be hidden in reports – go and find out what they're doing and what they're worried about!

2

Invest time in understanding your supply chain

Suppliers are vulnerable from cyber attacks too. We need to be really good consumers of services we buy – understanding what we are buying, how it powers our ICS and how we plan for resilience and continuity if key suppliers' services are unavailable. ICSs need to work in partnership with suppliers to stay safer.

- Do you understand how your ICS is powered? How data flows (or doesn't) around your services? What will be impacted if key suppliers are unable to provide their services for an extended period?
- Do you understand where your services are hosted and why, and what that means for the security of your ICS?
- Procurement is a lever. How can you, at an ICS level, leverage the money you're spending collectively to shape the market to provide modern secure services?
- What do you expect from your suppliers in terms of cyber response capacity and skills building in your system for cyber resilience – how can they contribute to a stronger system?

3

Share skills and expertise system-wide, share your assets system-wide

Recruitment is a challenge for all ICSs, particularly finding people with the right skills and expertise in cyber. Some ICSs are already sharing chief information officer or chief security officer roles between organisations to boost skills, knowledge and capability. Done well this can be an effective use of limited resources.

- Where are the opportunities to be creative about where you can share existing skills and experience and create cyber roles across the ICS?
- How are you supporting different organisations in your ICS such as the voluntary sector, who are often key in supporting care pathways?
- How well-placed you are as a health and social care system to step in and support smaller partners if they were attacked? How aligned and clear are your business continuity plans?

4

Challenge your system to share learning openly

You will already be monitoring all of the near misses, prevented attacks and other cyber incidents in your system – that's just good practice. And cyber is almost certainly high up on your risk register. But how can you challenge yourselves to be more open about what's happened or almost happened so that others can learn from you? Those who attack are sharing ransomware code, vulnerabilities and opportunities with each other – you will be better placed to respond to these threats if you share your experiences too.

- How do you currently surface near misses and prevented attacks? What discussions do you have at board level? How is the information shared and discussed? How could it be more open and engaging?
- Do you have the right tools to spot vulnerabilities and sufficient resources to manage the workload they generate?
- How is cyber presented on your board governance risk register? What is the quality of the conversations about learning?
- ICS leaders tell us that they sometimes feel intimidated by cyber, digital and technology. How can you make it easy and comfortable to talk about this topic in a way that encourages questions and contributions from everyone?

5

Don't underestimate the importance of building trusted relationships, support and collaboration

An attack on one organisation is likely to impact the whole of the ICS system. To respond effectively you will need to be able to support each other. Building strong relationships now means that they will be there when you need them. To do this you need to develop a culture that practises collaboration and supports rather than blames. This will be a mixture of informal relationships and building more formal resilience into your system through effective governance and processes.

- How are you creating space for people to collaborate, even when the system is under pressure?
- How strong is your culture of continuous improvement? Do you use peer review, good practice sharing and open conversations to learn from each other and from failure?
- How might you use audit and inspections as a service to help you get better as a system? Often these are seen as tick box exercises, but used well they can help systems learn and improve.

Further resources

National Cyber Security Centre *Cyber Security Toolkit for Boards*

National Cyber Security Centre *Ransomware, extortion and the cyber crime ecosystem*

NHS England *Cyber security guide for non-executive directors*

Our offer

The Digital ICS programme is a free support offer designed to support all integrated care board and integrated care system leaders to better harness digital transformation to enable delivery of system ambitions.

The programme is commissioned by NHS England as part of their NHS Digital Academy and delivered by NHS Providers in partnership with NHS Confederation and Public Digital.

Our bespoke leadership development sessions support ICS leaders in building confidence and understanding on digital transformation.

Please contact us at digital.ics@nhsproviders.org to find out more.

@NHSProviders
www.nhsproviders.org

NHS Providers · NHS Confederation · public digital · NHS