bcs The Chartered Institute for IT

60 CELEBRATING SIXTY YEARS 1957 - 2017

Making IT good for society

Blueprint for **CYBER SECURITY** in HEALTH AND CARE

June 2017

bcs.org/blueprint

'In health and care we have dedicated digital teams striving to protect our patients and public. I believe it is right to recognise the good work done in preventing the attacks and everyone who had worked tirelessly to minimise disruption. We need to build on that with collective input from those who care about protecting the public from cyber threats. That's why I support the **Blueprint for Cyber Security in Health and Care**.'

Andy Kinnear Chair **BCS Health and Care**

Supporting partners

Barnardo's
BT
Digital Health & Care Institute Scotland
IBM
The Institute of Engineering and Technology
Information Systems Security Association
Institute of Measurement and Control
Microsoft
NHS Wales
Patients Association
Royal College of Nursing
Society of Occupational Medicine

Andy Kinnear Chair of Health and Care Executive Committee **BCS**
Dr Reza Alavi Chair of Information Risk Management and Assurance Specialist Group **BCS**
Julian Schwarzenbach Chair of Data Centre Specialist Group **BCS**
Gareth Niblett Chair of Information Security Specialist Group **BCS**
Sarith Chandra Chair of Young Person Information Security Group **BCS**
Sharon Levy Chair of Health and Care Scotland Specialist Group **BCS**

Adrian Winckles Course Leader in Information Security and Forensic Computing **Anglia Ruskin University**
Professor William Buchanan Professor of Computing **Edinburgh Napier University**

'As a technology company, Microsoft has a special responsibility to address cybersecurity issues and we fully support the **Blueprint for Cyber Security in Health and Care** as a means to provide a benchmark in cybersecurity best practice. Across the tech sector, advances are being made which are making important contributions in the fight against cybersecurity threats, but more action is needed, and it is needed now. It's important that lessons are taken from previous incidents and applied to strengthen our collective response and capabilities, with the tech industry, customers, and governments working together to protect against cybersecurity threats.'

Hugh Milward Director, Corporate, External and Legal Affairs **Microsoft UK**

Executive summary

Today we face a very different environment in the digital world; the threats have changed, and the proliferation of digital technology has made the impact much more severe and system-wide when things go wrong. The 'Wannacry' ransomware demand that hit the NHS in May 2017 was a relatively small attack, and NHS professionals of all kinds worked tirelessly to ensure that any impacts on the public were minimal. Service-affecting issues across all kinds of organisations happen all the time; what made this unique was that NHS organisations were, in unusually large numbers, diverting ambulances and cancelling treatments. This has resulted in a new public awareness of the risks that the NHS and other organisations face.

Across government and the political sphere, cyber risks are often well understood, and work has been underway to build a more coherent and organised profession. Occurrences like 'Wannacry' have shown us that we need to accelerate and upgrade our collective response, now.

Fed-IP
As a professional body we have been working hard with our members in the health and care communities for a number of years to unite communities to support one another in our collective mission. This culminated in the launch, in May 2017 of a coalition of ten professional bodies involved in health and care informatics, who have come together with one aim; to ensure that patient outcomes are at the centre of their work.

Involving the professional
And now we're accelerating the extension of that community and convening the broader professional community; the individual professionals working across many different sectors who come together through a number of professional institutions. Our dual aim is to consult with and involve the professional community and their institutions along with patient organisations and broader stakeholders, to ensure that we have the right response.

We have been in contact with those working inside and out of the public sector, our colleagues working on relevant NHS policy and academic experts. We have the start of a broad coalition of organisations that wish to work together to build a cyber-safe NHS. All of these individuals and organisations recognise that an approach built on partnerships, sharing and mutual accountability is essential.

We know that sometimes securing an organisation will mean spending more money, but sometimes it will not. Boards need to be equipped to ask whether there is an appropriate cyber security plan in place and working, and they need to know who to ask it of. And those who are asked need to know how to answer... if this is in place we have a system that works. We do not believe that this is controversial or at its heart a politically-differentiated matter, but a simple case of professional collaboration. This is not in conflict with existing government or NHS programmes or priorities, but we also need the public's voice to be heard on this issue, to hold us all to account and to understand their role.

Accountable to the public
All of our partners involved here believe that digital technology should be safe and beneficial, and for the most part it is. We believe that our first duty is to the public, and we can only meet that duty if we collaborate and share. We will play our part, and we will be accountable to the public for keeping them safe as best we can.

'At BT we believe that critical health and care services must be protected from cyber-attack. We pledge our support for this roadmap for a cyber-safe NHS, extending our professional support, shared good practice, threat intelligence and resources. We'll contribute to developing the roadmap and collaborate to enhance NHS cyber security.'

Jason Hall Director – NHS Digital **BT Business and Public Sector**

'Cybersecurity is vitally important to patients, and will become ever more so. It almost goes without saying that people must feel confident in the security of their personal data. But at least as important is that we are able to seize the opportunities presented by digital technology to enable patients to take control of their care.'

John Kell Head of Policy **The Patients Association**

Blueprint for **Cyber Security** in Health and Care

Our vision is a world properly protected from cyber threat. It is not acceptable that where good practice exists, it is not used – especially where lives are put in danger. This is a systemic issue, and we need a systemic solution. This blueprint sets out how we can deliver that solution, starting in health and care.

Our goal
Prevent harm to the public where established cyber security good practice could stop it.

Why?
The purpose of our existence, our professional membership, and our place in society demands that we set out such a vision.

Our focus
We have a collective obligation to ensure that the public can trust NHS organisations to be safe and available, properly protected from cyber threats.

How we will deliver that
By building a willing coalition of those who share this goal to come together with urgency to set out a roadmap that turns this vision into reality.

Who can help us?

We are calling for:

POLICY MAKERS to commit to engaging in dialogue and support the policy actions that are required to deliver the roadmap.

PROFESSIONAL INSTITUTIONS to come together and build shared solutions; recognising that there are multiple professional communities that need to be involved, and that collaboration is essential.

PARTNER ORGANISATIONS to lend their support by participating in the development of the roadmap, and encouraging their professional teams to take an active role in the wider community.

PROFESSIONALS to get involved in their community and visibly declare their support for each other, and to play their role in taking responsibility for protecting the public.

THE PUBLIC to demand from all of us that we meet their needs and protect their interests, and hold us to account for doing so.

Show your support **www.bcs.org/blueprint**

Our **draft roadmap** for a cyber-safe NHS

By the end of 2017 we will have:

- Defined the role of NHS organisational boards across the UK, and IT / cyber professionals in the NHS, what they can expect from each other, and what the public can expect of them.
- This will result in:
  - Clear standards of practice for NHS organisations' boards
  - Standards for accreditation of relevant professionals to deliver for boards
  - A public and professional consultation on the above, to ensure it meets the needs of other health and care professionals and the general public
- Begun the first tranche of courses for digital leaders, working with programmes across the UK such as the NHS Digital Academy.
- A clear, costed and resourced plan to deliver the 2020 roadmap.

By the end of 2018 we will have:

- The first tranche of professionals across health and care, and other sectors as far as possible, qualifying and registering as professionally competent.
- Begun the roll-out of advice and guidance to NHS boards to ensure they understand their responsibilities and how to make use of registered professionals to meet their obligations.
- Commissioned independent research and studies to look at how NHS organisations are changing and need to change to fully implement these changes.
- Created the frameworks and processes to ensure that academic research on security and practice, along with real-life experience from registered practitioners, forms the basis of future developments and standards, and is a requirement for professionals to remain registered.

By the end of 2019 we will have:

- Expanded the number of professionals undertaking qualifications and registering, to meet the needs of the full estate of NHS organisations.
- Learned from and implemented changes arising from our initial experiences.
- Completed the induction of NHS boards and relevant organisations, so they enter 2020 with a clear understanding of their responsibilities, and plans in place.

In 2020 we will be able to:

- Assure the public that NHS organisations are equipped to meet current and future challenges.
- Assure the public that there are accountable professionals keeping the NHS safe from cyber attacks.
- Highlight with full transparency where there are gaps.
- Learn from future incidents in a structured way, and anticipate threats reliably.

'Effective cyber security initiatives require sufficient coordination between risk management process, well-qualified people, strengthened technology and dependable assurance processes. This blueprint provides a road-map for achieving this coordinated objective.'

Dr Reza Alavi Chairman **BCS IRMA (Information Risk Management and Assurance Group)**

Why the **NHS**?

Cyber security threats affect every part of society; including the entire public sector, corporations small and large, everywhere that computer systems are used. However, the role the NHS plays in our lives and the nature of the threat to it puts this as the first priority.

Other sectors must follow in close succession, but without focus we will achieve nothing. The NHS is also at a critical juncture in the development of the IT profession within health, and the use of digital in the delivery of health and care.

Why not eliminate all cyber threats?
Our vision is a world free of cyber threats, it is not currently possible to eliminate all cyber threats. Instead, we are looking to eliminate the threats from poor practice, and create a supported professional community that can be relied upon to deliver known good practice, and to up the pace of development of good practice commensurate with the pace of the threat environment. In other words, our goal is not to protect against the unknown, but against the known – and as new unknown threats emerge, to ensure that they are known and dealt with rapidly.

This is analogous with the safety of cars. We cannot eliminate deaths from accidents, but we can make sure that cars are maintained and in good order, and that when an accident occurs the design minimises the harm. Over time, we may eliminate road deaths as our technology and approach improve.

Over time, we may eliminate cyber threats in a similar way, but total elimination of cyber threats is simply not possible at the end of any realistic roadmap.

'This isn't about telling people what to do, but it's about supporting them; bringing together communities with knowledge and expertise to enable others.'

Paul Newman Head of Information Technology **Royal College of Nursing**

The **Pledge**

PROFESSIONAL INSTITUTIONS IN CYBER SECURITY

We **believe** that we have a responsibility to ensure the public's best interests are at the heart of professional cyber security practice. We believe this is important in all sectors, and in particular where lives and wellbeing are at risk, such as in health and care. We will work together as part of a professional community, putting the public first, to ensure public confidence and trust is met with the highest standard of professional practice. We will champion the development of a shared roadmap that connects the responsibilities of organisations and the responsibilities of individual professionals so that there is a clear accountability and continuous improvement.

PROFESSIONAL INSTITUTIONS IN HEALTH AND CARE

We **believe** that:
1. The way we use information and technology to deliver health and care has a critical impact on citizens and our communities
2. The best is only possible when everyone puts our citizens and communities first, and works together
3. All those involved in health and care owe a duty to our communities to strive together for the very best for them, and in turn need to be supported and recognised when they do.

We will work together with cyber security institutions, putting the public first, to ensure that health and care informaticians, security and information governance specialists, use good practice supported by the best from all sectors available to us.

PARTNER ORGANISATIONS

We **believe** a health and care environment that is secure from cyber threat matters to all of us.
We **support** a roadmap to a cyber-safe NHS, and we will encourage our professional teams to participate as part of the community, sharing good practice and supporting colleagues. We will review and contribute to the development of the roadmap.

PROFESSIONALS (HEALTH AND CARE)

As a professional working to design, deliver, manage or lead in health and care informatics, I will:
1. Actively promote and demonstrate my commitment to putting communities first in health and care, and set an expectation that others do the same
2. Seek to learn, develop and share what delivers the best health and care
3. Not tolerate professional or organisational rivalries that conflict with what our communities need
4. Play an active role in my own professional community, and multi-disciplinary communities that support these aims.

PROFESSIONALS (CYBER SECURITY)

As a professional working in cyber security, I will:
1. Actively promote and demonstrate my commitment to putting the public first, and set an expectation that others do the same
2. Seek to learn, develop and share what delivers the best health and care
3. Not tolerate professional or organisational rivalries that conflict with what our the general public needs
4. Play an active role in my own professional community, and multi-disciplinary communities that support these aims

THE GENERAL PUBLIC

I **support** professionals who put the public need first. I call on policy makers, professional institutions and all those involved in securing vital services and protecting us to work together for the good of all of us.

BCS, The Chartered Institute for IT is here to make IT good for society. We promote wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

Our 73,000 strong membership includes practitioners, businesses, academics and students in the UK and internationally. We deliver a range of professional development tools for practitioners and employees. A leading IT qualification body, we offer a range of widely recognised qualifications.

BCS Health and Care resources

Overview of BCS Health and Care programme
www.bcs.org/healthandcare

Health and Care Executive member profiles
www.bcs.org/healthandcareprofiles

Recent IT impact event, featuring former BCS Health and Care Chair, Matthew Swindells
www.bcs.org/itimpacthealth

BCS The Chartered Institute for IT
First Floor Block D North Star House North Star Avenue Swindon SN2 1FA
T +44 (0) 1793 417 655 **bcs.org/healthandcare**

If you require this document in accessible format please call +44 (0) 1793 417 600