Cyber Security Strategy

Content

Introduction 3

Strategic Context 3

I. Threats and Risks 3

II. Vulnerabilities 4

Our Response 5

I. Mission and Vision 5

II. Principles 5

III. Roles and Responsibilities 5

Our Plan 6

Objective 1 – Defend 6

Objective 2 - Deter 7

Objective 3 – Develop 8

Objective 4 – Respond 8

NHS Digital 9

Measuring Success 9

I. Outcomes 9

II. Monitoring and Assurance 9

Appendix A: 10 steps to Cyber Security 9

Appendix B: Glossary 11

Introduction

Patients, service users and staff have a right to expect that information about them is held securely. Protecting information held on computers is called cyber security. Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber-attacks. Effective cyber security reduces the risk of cyber-attacks; protects organisations from the unauthorised exploitation of systems, networks and technologies, and data theft; and ensures robust response plans are in place.

As the Trust has become primarily digitised, both the protection of data and keeping information systems in use have added to the need to ensure an effective cyber security strategy.

This Strategy is based on and uses wording directly from the HM Government Cyber Security Strategy.

Strategic Context

Cyber crime is now the largest reported crime in the UK. New technologies and applications have come to the fore and greater uptake of internet-based technologies worldwide, in particular in developing countries, has offered increasing opportunities for economic and social development. These developments have brought, or will bring, significant advantages to connected societies such as ours. But as our reliance on networks grows, so do the opportunities for those who would seek to compromise our systems and data. Equally, the geopolitical landscape has changed. Malicious cyber activity knows no international boundaries. State actors are experimenting with offensive cyber capabilities. Cyber criminals are broadening their efforts and expanding their strategic modus operandi to achieve higher value pay-outs from UK citizens, organisations and institutions. Terrorists, and their sympathisers, are conducting low-level attacks and aspire to carry out more significant acts. This chapter sets out our assessment of the nature of these threats, our vulnerabilities and how these continue to evolve.

I. Threats and Risks

There are numerous threats and risks to the NHS, which threaten Information Systems and IT services. This in turn could be a risk to patient data and the Trust's reputation.

Cyber-dependent crimes - Crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity).

Cyber-enabled crimes - Traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

Terrorists – Terrorist groups continue to aspire to conduct damaging cyber activity. The current technical capability of terrorists is judged to be low. Nonetheless the impact of even

low-capability activity to date has been disproportionately high: simple defacements and doxing activity (where hacked personal details are 'leaked' online) enable terrorist groups and their supporters to attract media attention and intimidate their victims**.**

Hacktivists - Hacktivist groups are decentralised and issue-orientated. They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts. While the majority of hacktivist cyber activity is disruptive in nature, more able hacktivists have been able to inflict greater and lasting damage on their victims

II. Vulnerabilities

The NHS has various vulnerabilities which need managing to mitigate risk of a cyber-attack. The consequence of failing to do so, could be corrupt information systems or data, where patient appointments need to be cancelled or patient diagnostic results are delayed due to information systems being unavailable.

An expanding range of devices - When the last National Cyber Security Strategy was published most people conceived of cyber security through the prism of protecting devices such as their desktop computer or laptop. Since then the Internet has become increasingly integrated into our daily lives in ways we are largely oblivious to. This creates new opportunities for exploitation and increases the potential impact of attacks which have the potential to cause physical damage, injury to persons and, in a worst case scenario, death. Therefore, we are no longer just vulnerable to cyber harms caused by the lack of cyber security on our own devices but by threats to the interconnected systems that are fundamental to our society, health and welfare.

Poor cyber hygiene and compliance - Awareness of technical vulnerabilities in software and networks, and the need for cyber hygiene has undoubtedly increased over the past five years. This is in part a consequence of initiatives like the Government's '10 Steps to Cyber Security', which the Trust benchmarks against, but also due to the increased public profile of major cyber incidents affecting governments and corporations. Cyber-attacks are not necessarily sophisticated or inevitable and are often the result of exploited – but easily rectifiable and, often, preventable vulnerabilities.

Insufficient training and skills – We lack the skills and knowledge to meet our cyber security needs across the public sector as a whole. In the Trust many staff members are not cyber security aware and do not understand their responsibilities. The public is also insufficiently cyber aware.

Legacy and unpatched systems - Many organisations continue to use vulnerable legacy systems until their next IT upgrade. Software on these systems often rely on older, unpatched versions. These older versions often suffer from vulnerabilities that attackers look for and have the tools to exploit. An additional issue is the use by some organisations of unsupported software, for which patching regimes do not exist.

Hosted systems - The NHS is reliant on vendors who provide cloud based hosted solutions for the NHS. The Trust is dependent on the cyber security of its suppliers. Every organisation much seek assurance that the vendors solutions are patched to the latest specifications to mitigate any risk.

Partners - The NHS also has interoperability with partner NHS organisations to care for our patients. The Trust is dependent on the cyber security of its partners. There is a requirement to seek assurance from each other that IT information systems are kept secure.

Our Response

To ensure the Trust is kept as safe as it can be from a cyber-attack the Mission and Vision, Principles and Roles and Responsibilities is outlined below. The approach and monitoring aspects of the plan are detailed in the following section.

I. Mission and Vision

Taking into account all the current threat, risks and vulnerabilities, the Trust will use state of the art, current security tools and security-trained informatics skills to ensure the Trust is as safe as it can be from cyber security attacks. It will ensure all staff have the correct information and knowledge to play their part in protecting the Trust

The Trust currently takes a risk adverse position in relation to cyber security. For example, the Trust locks down external IT network ports by default and only opens them on request, after a risk assessment has been carried out.

The Trust recognises that a cyber-attack or threat at some point will require a response. The Trust will have a robust response plan in the case of a cyber-attack or threat.

II. Principles

The Trust will follow the following principles to ensure we are safe from cyber criminals:

- We will treat a cyber-attack as seriously as we would an equivalent conventional attack and we will defend ourselves as necessary;
- We will preserve and protect our patients and staff privacy; and
- We will not accept significant risk being posed to the Trust as a whole as a result of vendors and partners or other organisations failing to take the steps needed to manage cyber threats.

III. Roles and Responsibilities

Everybody has a role to play in cyber security, the responsibilities of each group of staff and bodies are listed underneath.

All Staff – Will ensure they pass the annual information governance training which includes cyber security and uses these skills in every part of their work.

Informatics Staff – Will ensure the Trust is kept safe, by ensuring monitoring tools are kept up to date and the correct skills to identify and respond to threats are always current. Informatics will continually monitor Trust staff compliance with mandatory security training.

Vendors – Must follow the NHS Digital advice and guidance. All suppliers must have or be working towards the ISO27001 accreditation to provide assurance they have systems and processes in place for security.

Partners – Must take cyber security seriously and implement processes and procedures to ensure they do not put any shared services at risk.

Digital Governance - Will monitor the age of equipment and versions behind of software as these are critical elements of ensuring a cyber secure position

Information Governance - Will monitor the Trust's current cyber security position and escalate where necessary. The Sub-Committee will hold the implementation of this strategy to account and seek assurance that there is no deviance.

NHS Digital -This is a national body that issues weekly advice and guidance on the latest cyber –security threats and are the NHS experts in terms of cyber security.

Care Quality Commission - Can visit the Trust to audit the Trust's current cyber security position and issue directives. This can be an unannounced audit.

Our Plan

The Trust will use a number of technologies and skills to ensure all information systems and data is kept secure at all times. The Trust will respond quickly and effectively to cyber-attacks and mitigate all risks to ensure the Trust can care for their patients at all times.

The Trust will use four objectives to ensure the Mission and Vision are met.

Objective 1 – Defend

The Informatics Department will use a range of technologies to ensure any potential cyber security are identified and blocked before any adverse effect to the Trust.

Approach

The Trust will:

- Use dual high rated vendor, high-end firewalls
- Use the expertise of highly rated vendors to automatically update against any threats.
- Use a threat management appliance.
- Use automated blocking of suspect web sites.
- Impose restrictions on web sites not properly categorised by our firewall vendor Restrict access to end-point devices. to prevent any peer to peer file sharing.
- Use email security, including anti-spam measures.

- Roles and Responsibilities of key IT staff will defined and agreed.
- Trust Opel plans will include the “go dark” protocol to efficiently respond to a threat.

Monitoring

The Trust will monitor by:

- Continuously reviewing IT network traffic and set triggers to identify risks.
- Have real time alerts for potential cyber risks within systems used for email and internet usage.

Objective 2 - Deter

The Informatics Department manage cyber security risks by using controls and IT technical user policies to mitigate risk, to ensure the routes to any potential cyber-attack are mitigated.

Approach

Informatics will ensure the following are in place:

- Restriction of public connection to the wireless network
- End user devices will be locked down to prevent unauthorised access
- Restriction of the downloading of applications by staff
- Anti-virus will be rolled out to the latest release
- Communication rooms & data centres are secure at all times
- Patch end user devices with vendor security updates within three weeks of release
- Patch servers with vendor security updates, three weeks from release for mission critical systems and 12 weeks for the remainder
- Encrypt all end-point devices and anti-virus protection.

Monitoring

The Trust will monitor by:

- The Service Level agreement for patching in the monthly Information Governance report
- All entry into locked communications room provided by authorised staff and recorded in a log book
- Anti-virus alerts monitoring.

Objective 3 – Develop

The Trust will continually develop processes and staff to keep the Trust safe.

Approach

The Trust will have constantly challenging and developing plans and skills including:

- Robust and approved cyber incident plans will be in place
- Robust knowledge sharing through NHS Digital Care Cert and Care Cert Collect services
- Achieving a 95% compliance rate with Information Governance training, which includes cyber security
- Ensuring key IT personnel have relevant Security training (such as Certified Information Systems Security Professional – CISSP or Systems Security Certified Practitioner - SSCP).

Monitoring

The Trust will monitor by:

- Scheduled review of cyber plans by the Business Continuity Group
- Staff awareness will be continuously monitored using various campaigns e.g. a dummy email to say reset your password.
- IT staff knowledge and skills will be tracked through the Time to Talk appraisal process, which tracks staff mandatory training compliance
- An action plan to track the Trust's compliance with the "10 steps to Cyber Security" protocol

Objective 4 – Respond

It us important the Trust has robust plans to respond to any cyber risks or cyber attacks

Approach

To ensure the Trust can respond quickly and effectively to any cyber security risk we will:

- Have robust response plans with no single points of failure in terms of staffing
- Have a "go dark" process to mitigate any risks of a cyber attack

- Have comprehensive business continuity plans to ensure patient risk is mitigated when Information Systems are unavailable,

Monitoring

The Trust will monitor by:

- All plans will be constantly evolving to ensure they are fit for purpose, which will be monitored and measured
- Conducting an cyber testing and any lessons learnt updated into plans/procedures

NHS Digital

NHS Digital is a national NHS body who oversees national policy for information technology systems and services. They are the guardians of patient data, making sure it is protected and handled securely. NHS Digital is the central body that circulates Cyber Security bulletins, known as CareCert bulletin, which all NHS bodies must review and take any actions as necessary. They also offer both technical and staff training for staff in NHS Trust's to raise skills and awareness of cyber security risks.

Measuring Success

The Trust needs to ensure this strategy is successful and the implementation must be tracked for assurance the Trust are keeping patient data safe at all times.

I. Outcomes

The Trust will consider this strategy a success by using the following indicators:

- Identification of all cyber threats before data is breached
- Information systems are patched within a timely manner
- Responded to all cyber threats using the approved process
- 95% of all staff know their responsibilities by completing annual Information Governance training.

II. Monitoring and Assurance

The outcomes will be monitored by:

- The Information Governance group
- Digital Governance, concerning age of equipment

Appendix A: 10 steps to Cyber Security

Appendix B: Glossary

Action Fraud – the UK's national fraud and internet crime reporting centre, providing a central point of contact for the public and businesses.

Active Cyber Defence (ACD) – the principle of implementing security measures to strengthen the security of a network or system to make it more robust against attack.

Anonymisation – the use of cryptographic anonymity tools to hide or mask one's identity on the Internet.

Authentication – the process of verifying the identity, or other attributes of a user, process or device.

Automated system verification – measures to ensure that software and hardware are working as expected, and without errors.

Autonomous System – a collection of IP networks for which the routing is under the control of a specific entity or domain.

Big data – data sets which are too big to process and manage with commodity software tools in a timely way, and require bespoke processing capabilities to manage their volumes, speed of delivery and multiplicity of sources.

Bitcoin – a digital currency and payment system.

Commodity malware – malware that is widely available for purchase, or free download, which is not customised and is used by a wide range of different threat actors.

Computer Network Exploitation (CNE) – cyber espionage; the use of a computer network to infiltrate a target computer network and gather intelligence.

Cyber Crime marketplace – the totality of products and services that support the cyber crime ecosystem.

Cryptography – the science or study of analysing and deciphering codes and ciphers; cryptanalysis.

Cyber-attack – deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm.

Cyber crime – cyber-dependent crime (crimes that can only be committed through the use of ICT devices, where the devices are both the tool for committing the crime and the target of the crime); or cyber–enabled crime (crimes that may be committed without ICT devices, like financial fraud, but are changed significantly by use of ICT in terms of scale and reach).

Cyber ecosystem – the totality of interconnected infrastructure, persons, processes, data, information and communications technologies, along with the environment and conditions that influence those interactions.

Cyber incident – an occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may require a response action to mitigate the consequences.

CyberInvest – a £6.5m industry and government scheme to support cutting-edge cyber security research and protect the UK in cyberspace.

Cyber-physical system – systems with integrated computational and physical components; 'smart' systems.

Cyber resilience – the overall ability of systems and organisations to withstand cyber events and, where harm is caused, recover from them.

Cyber security – the protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.

Cyber Security Challenge – competitions encouraging people to test their skills and to consider a career in cyber.

Cyberspace – the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet-connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept.

Cyber threat – anything capable of compromising the security of, or causing harm to, information systems and internet-connected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means.

Data breach – the unauthorised movement or disclosure of information on a network to a party who is not authorised to have access to, or see, the information.

Domain – a domain name locates an organisation or other entity on the Internet and corresponds to an Internet Protocol (IP) address.

Domain Name System (DNS) – a naming system for computers and network services based on a hierarchy of domains.

Doxing – the practice of researching, or hacking, an individual's personally identifiable information on the Internet, then publishing it.

e-commerce – electronic commerce. Trade conducted, or facilitated by, the Internet.

Encryption – cryptographic transformation of data (called ‘plaintext’) into a form (called ‘cipher text’) that conceals the data’s original meaning, to prevent it from being known or used.

Horizon scanning – a systematic examination of information to identify potential threats, risks, emerging issues and opportunities allowing for better preparedness and the incorporation of mitigation and exploitation into the policy-making process.

Incident management – the management and coordination of activities to investigate, and remediate, an actual or potential occurrence of an adverse cyber event that may compromise or cause harm to a system or network.

Incident response – the activities that address the short-term, direct effects of an incident, and may also support short-term recovery.

Industrial Control System (ICS) – an information system used to control industrial processes, such as manufacturing, product handling, production and distribution, or to control infrastructure assets.

Industrial Internet of Things (IIoT) – the use of Internet of Things technologies in manufacturing and industry.

Insider – someone who has trusted access to the data and information systems of an organisation and poses an intentional, accidental or unconscious cyber threat.

Integrity – the property that information has not been changed accidentally, or deliberately, and is accurate and complete.

Internet – a global computer network, providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.

Internet of Things – the totality of devices, vehicles, buildings and other items embedded with electronics, software and sensors that communicate and exchange data over the Internet.

Malware – malicious software, or code. Malware includes viruses, worms, Trojans and spyware.

Network (computer) – a collection of host computers, together with the sub-network or inter-network, through which they can exchange data.

Offensive cyber – the use of cyber capabilities to disrupt, deny, degrade or destroy computers networks and internet-connected devices.