TIAN
The Internal Audit Network

Cyber Security Newsletter

Welcome to the second TIAN Cyber Security Newsletter.

Our newsletters will aim to ensure readers are aware of cyber security topics and incidents particularly relevant to Health & Social Care.

In this edition:

About TIAN

The Internal Audit Network (TIAN) is a professional network of NHS based internal audit providers, bringing together collective thinking to add greater value to our clients.

TIAN is a membership network with a unique understanding and insight of the public sector, working with an NHS ethos aligned to public sector values. Our collective positioning across England and strong NHS client base continues to support valuable benchmarking and sharing of best practice.

The articles within this issue were submitted by TIAN members Audit North, 360 Assurance and the Information Security & Assurance Service of West Midlands Ambulance Service NHS Foundation Trust (ISAS) respectively.

Information Security & Assurance Service

TIAN provides expert cyber security and wider IT assurance services to numerous public sector organisations throughout the UK. Our client base extends beyond the NHS to Further Education Colleges as well as national and local government.

For further information please contact cybersec@tian.org.uk or visit our website at www.tian.org.uk.

Issue 2, November 2016

1. The General Data Protection Regulation (GDPR)

Overview

Even though the UK voted to leave the EU, the Government, working with the Information Commissioner's Office (ICO), now needs to consider the impact of the GDPR and its impact on data protection reform in the UK as necessary.

Although many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act 1998 (DPA), there are new elements and significant enhancements, so organisations will have to do some things for the first time and some things differently.

Forward Planning

It is essential that organisations start planning their approach to GDPR compliance as early as possible in order to gain 'buy in' from key individuals, including the Board, as particularly in large, complex organisations there could be significant budgetary, IT, personnel, governance and communication implications.

Individuals Rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA. Full details of the rights are available at www.dpreform.org.uk. Lawful processing becomes more of an issue under the GDPR because the legal basis for processing has an effect on individuals' rights.

Organisation Accountability and Governance

While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. Organisations are expected to put into place comprehensive but proportionate governance measures, which should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

Continued... The General Data Protection Regulation

What to do first

The Information Commissioner's Office has produced a 12 step Checklist to highlight some of the key areas you need to start considering, key changes likely to impact NHS organisations include:

1. Update privacy notices in time for GDPR implementation.

2. Plan how the organisation will handle subject access requests within the new timescales.

3. Review how the organisation seeks, obtains and records consent.

4. Produce procedures to detect, report and investigate data security breaches.

5. Ensure Data Protection Impact Assessments and Data Protection by Design are in place.

6. Designate a Data Protection Officer.

What should I ask my Board?

1. Is my Board prepared for the transparency requirements of the GDPR, which include a new requirement, known as the ‘accountability’ principle?

2. Is my Board ready to demonstrate their accountability, including how they manage data protection as a corporate issue?

3. My Board is expected to put comprehensive but proportionate governance measures into place, to minimise the risk of breaches and uphold the protection of personal data – can they demonstrate this now?

4. Does our Data Protection Team have sufficient staff and skills to discharge our obligations under the GDPR?

Further information on data protection reform

The ICO have a new data protection reform website www.dpreform.org.uk where they will post information about the reform of data protection legislation, including under the GDPR and the Directive. You are advised to check it for updates regularly.

2. 2016 - Cyber Incidents

If you Google 'healthcare cyber-attack' you might be forgiven for thinking that it is only a problem in America. But when America sneezes the world catches a cold, and this was evidenced when the North Lincolnshire and Goole NHS Foundation Trust (NLAG) was infected by a 'virus'.

The virus (most likely ransomware) caused key NLAG clinical systems to be shutdown and also impacted partner organisation United Lincolnshire Hospitals NHS Trust (ULH) which shares 4 clinical systems with NLAG.

The incident, the worst reported to have hit the NHS, resulted in all but the most vital appointments being cancelled by NLAG with operations also cancelled in Lincoln, Grantham and Boston.

Derriford Hospital (Plymouth), East and North Hertfordshire NHS Trust and Papworth Hospital have also highlighted they received ransom remands following ransomware attacks, although have recovered reportedly without making any payment.

A recent FOI request to the NHS identified that 28 NHS trusts had suffered ransomware attacks in the last 12 months.

To date, cyber attacks do not appear to have directly caused death, but they have caused substantial disruption to staff, delays in discharges and cancellation of operations – at a time when the NHS is under strain, it can ill-afford further disruption to its critical IT systems. In addition to the NLAG incident The Royal Berkshire Hospital postponed numerous operations earlier this year, following a virus infection. The virus came as an attachment to an email, and was a variant of a known XP-virus. The incident, reported in the local media, did not appear to receive much public sympathy, with numerous commentators astounded that the Trust was still operating XP systems in 2016. Areas to focus upon to prevent and subsequently limit malicious code infections include:

- System backups including their accessibility – consider offline backup media.
- System and network logical segregation - avoid 'flat' networks where possible.
- Minimise user operating system permissions and use of 'admin' accounts.
- Raise user awareness via training and pro-active self-phishing exercises.
- Anti-virus software deployment and intrusion detection systems.

Continued... 2016 - Cyber Incidents

The Healthcare Efficiency Through Technology show in London (28th September 2016) reported that the CareCERT programme is also uncovering widespread and frequent attacks on the NHS. An unnamed NHS hospital was recently targeted by a hacker through windows XP. The hacker infected 60 servers and used them to send 2 million spam emails in an attack that "wasn't sophisticated – this was a bedroom hacker".

Organisations should not take much comfort from being on N3 – 0.3% of all traffic over this network is estimated to be malicious, and 60% of all email sent to NHS mail 2 is blocked. N3 should be treated as a private but untrusted network.

Further afield in March it was reported that Medstar – a United States company operating 10 hospitals in the Baltimore Region was forced to shut down its entire IT network and revert to paper records. The chain, which had serviced more than 4.5 million patients in 2015 was reportedly forced to turn away patients following the attack, and its 35,000 staff were left unable to access emails or look up digital patient records.

Politico.com highlighted that the Obama administration pushed out a $35 billion incentive programme to convert to digital records. This encouraged organisations to move to digital records before they were ready, resulting in systems containing vulnerabilities and staff without the technical skills to deal with them. It is not enough to rely on security systems to counter known risks; new zero day attacks were reported on average every week during 2015, a position that is likely to only get worse. Healthcare organisations are particularly vulnerable because of their complex and diverse technical environments. Cyber strategies are designed around detecting and keeping out bugs, but how many devices ranging from a bedside monitor to a drug pump to a fax machine create a potential backdoor to a hacker?

3. Data Security and Governance – A Step Change

In July 2016 a number of publications pertaining to the safe use and protection of personal health care information were published. Whilst the publications are in the context of healthcare data the principles apply equally to all personal data stored and processed by the NHS.

The **CQC Policy Statement** on Information Security and Governance expounds the commitment to the principles of confidentiality, integrity and availability in the management of information systems and data. The document details the limited arrangements CQC currently deploys in relation to regulating Information Governance (IG) and identifies actions by the CQC in light of the proposed data standards such as:

1. Checking internal and external validation against standards.

2. Ensuring CQC inspectors are appropriately trained; and

3. Considering whether organisations work collaboratively.

Safe Data Safe Care reflects the importance of data security and details how new National Data Guardian (NDG) Data Security Standards can be assured via CQC inspections. The review draws on existing Information Governance Toolkit requirements, the Cyber Essentials Scheme and the results from penetration testing of NHS information systems. The publication highlights failure to:

1. Obtain independent validation of compliance with policies and procedures.

2. Learn from breaches and incidents and benchmark amongst similar organisations.

3. Comprehensively train staff including SIROs and Caldicott Guardians.

4. Secure records in transit.

5. Ensure the IG Toolkit is up to date and fair in its scoring.

Continued... Data Security and Governance – A Step Change

The report made six recommendations covering the areas of Leadership, Staff Training, Systems and Data Security Protocols, Internal & External Compliance Testing, Systems Design and the CQC assessment framework.

The NDG Data Security Standards are intended to apply to every organisation handling health and social care information, although the way that they apply will vary according to the type and size of organisation.   Leaders of organisations should commit to 10 new data security standards with commitment being demonstrated through independent and objective assurance.

The standards relate to 3 leadership obligations:

Leadership Obligation 1: People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Leadership Obligation 2: Process: Ensure the organisation pro-actively prevents data security breaches and responds appropriately to incidents or near misses.

Leadership Obligation 3: Technology: Ensure technology is secure and up-to-date.

TIAN recommends that client management:

1. Formally acknowledge Board level responsibility for Information Security (IS).

2. Undertake a high level stock-take of their current IS position.

3. Undertake a thorough risk assessment of all aspects of IS including the adequacy of training for the Caldicott Guardian and SIRO roles.

4. Receive formal reports regarding the validity of their IG Toolkit (or equivalent) submissions on an on-going basis (rather than annually as at the moment).

5. Receive assurances and independent assurance regarding data security.

6. Review current training content and uptake.

Our Information Security & Assurance Services

TIAN Information Security and Assurance teams provide services to clients throughout the UK and are available to assist you and your organisation in any number of specialist areas.

Our accredited teams provide clients with independent opinions and assurances regarding areas such as:

- Digital Forensics.
- Business Continuity.
- Emergency Preparedness and Disaster Recovery Planning.
- Configuration and Standard Build Assessment
- Penetration Testing
- Vulnerability Assessment
- Network and Infrastructure Resilience
- Compromise Monitoring
- IT Governance and Audit.
- Compliance with Legislation (e.g. Data Protection Act 1998).
- Standards Compliance (e.g. ISO27001, NHS IGT).
- Voice Over IP (VOIP) Security and Resilience.
- Cloud Computing.
- Security Event & Incident Monitoring.
- Network Design.
- Application Design.

For further information regarding any of our services please contact

cybersec@tian.org.uk

or visit

www.tian.org.uk.