Protect • Comply • Thrive

Can a cyber resilience programme secure your information systems *and* help achieve compliance?

www.itgovernance.co.uk

Introduction

The threat of cyber crime has grown exponentially as the digital revolution increases the role of technology in all aspects of life. Over the past few years, the healthcare industry has been one of the most affected by cyber crime, both in the number of cyber incidents and the impact that a loss of business functionality has on patients. In response to growing threats, new compliance parameters are being introduced from 2018.

This paper examines the cyber threats facing healthcare, including healthcare providers and the industry that supports the provision of care. It also considers the role of legislation in addressing the common causes of a breach and how useful compliance practices are in addressing threats.

Executive Summary

The Data Protection Act (DPA) has been the security framework for businesses that hold personal data since 1995. Although this has served admirably, it has become outdated, as shown by the rising impact of cyber crime and increasing cyber security incidents.

In response, the General Data Protection Regulation (GDPR), the EU Directive on Security of Network and Information Systems (NIS Directive) and the Data Security and Protection (DSP) Toolkit will come into force in 2018, each aiming to stop the rising threat of cyber crime and to mitigate threats. Having considered the different compliance requirements in silo, this paper will look at a more holistic approach to cyber security.

Historic Threats

Verizon[1] recently released its annual report, which examines global data breaches in 2016, both generally and specific to healthcare.

The report identifies the primary causes of data breaches:

Hacking and malware

From 2010 there has been little fluctuation in the threat of hacking and malware, and these remain the two primary causes of data breaches.

Social

Social refers to breaches that occur at a point of information sharing. This includes phishing attacks, bribery and business email compromise. Social attacks have increased dramatically from 2010 and are now the third most common cause of a breach.

Error and misuse

User error or misuse of privileges have remained consistently low across all industries, although both are significantly more prevalent in healthcare and the public sector than any other industry.

Physical

Physical theft of data is decreasing, probably because of the increased use of digital storage systems.

Healthcare-specific data

Healthcare saw 458 cyber security incidents worldwide in 2016, 72% of which were malware incidents. 296 of the incidents involved a confirmed data breach, representing 15% of total breaches worldwide.

Actors

Of the 296 cyber security incidents that resulted in a data breach, 68% involved an internal actor, 32% involved an external actor and 6% involved a partner. In some cases, the incident involved more than one type of actor.

Motivation

64% of the data breaches discovered were financially motivated, 23% were recreational and 7% motivated by a grudge. The remaining 6% had a range of other motivations.

Data

Of the 296 cyber security incidents that led to a data breach, 69% resulted in a loss of medical data, 33% resulted in a loss of personal data and 4% resulted in a loss of payment data. In some cases, the breach resulted in the loss of more than one type of data.

The report highlights that the changing digital landscape can have as much of an impact on the organisation's needs as the actual threats.

National Data Guardian for Health and Care Review [ii]

In June 2016, Dame Fiona Caldicott published a report that reviewed data security, and consent and opt-outs in healthcare. The review identified vulnerabilities in NHS systems and suggested improved security standards, which now form the framework of the DSP Toolkit.

Prioritisation and compliance were highlighted as concerns. The report found that the Information Governance (IG) Toolkit was seen as a "tick-box exercise", and that information security was often prioritised only if there was a threat or recent incident of a breach. The report highlighted the following common vulnerabilities:

Human vulnerabilities

Staff were seen as a cause for concern, with human behaviour highlighted as the leading cause of breaches. Informed and aware staff can prevent vulnerabilities from being exploited and are better prepared to report a breach and allow the impact to be minimised and mitigated.

Technical vulnerabilities

The report identified cases in which information security was included in the development of applications and systems, but the design of these security measures was not optimal for frontline functionality or delivery of care. This resulted in frontline 'workarounds' to bypass technical controls, which can be easily exploited by hackers.

Unencrypted devices are seen as a particular vulnerability because of the potential for loss or theft. The report also indicates that their use "[resulted] in a fine of £325,000 to a single NHS Trust".

The report also discovered technological vulnerabilities, including dormant accounts, default passwords and multiple logins from the same account.

The report encouraged the wider use of de-identified and anonymised data.

Care Quality Commission (CQC) Report [iii]

The CQC Report, released in July 2016, looked at data security against three measures: confidentiality, integrity and availability.

The report found widespread evidence of poor practice, which could have led to a data breach, despite the number of breaches being proportionally low with "533 data breaches in the year to 31 May 2015, in the context of 6.5 billion (digital) data transactions".

The report recommended six areas of improvement:

1. An organisation's senior management should take responsibility for information security.
2. Appropriate training should be provided to all staff.
3. Systems should avoid the need or ability for frontline staff to bypass technical controls.
4. Unsupported systems should be replaced as a matter of urgency.
5. Internal data security audits and external validation should be strengthened.
6. The CQC will amend its assessment framework to include data security management.

Causes of a breach

Broadly speaking, these reports found the main concerns facing information security in healthcare to be a combination of developing threats and persistent vulnerabilities:

Threats

Deliberate, malicious attacks continue to be a primary threat leading to data breaches in healthcare. The three most commons modes of attack are hacking, malware and social engineering.

Attacks can involve individuals or groups external to the organisation, or can be the work of 'malicious insiders'.

Vulnerabilities

Unencrypted devices are considered a threat as the loss or theft of these can lead to unauthorised access to systems and networks. Similarly, the use of non-anonymised big data sets can be a threat, particularly at the point in which these files are sent or shared.

Employees are one of the biggest vulnerabilities facing healthcare. Staff lacking awareness of their individual responsibility for information security is a catalyst for many breaches.

Impact

Business continuity is often affected by data breaches. Malicious actors often target healthcare organisations because they know that the information is valuable and that the targets may be unable to operate without access to the data.

Overview of legislation

The GDPR

The GDPR will come into effect in May 2018, extending the data rights of individuals in EU member states. New responsibilities under the GDPR include:

Consent

Consent must be "a freely given, specific, informed and unambiguous indication of the individual's wishes".

Rights of the individual

The GDPR solidifies and expands individuals' rights regarding how their data is used. The GDPR includes the right to be forgotten and the right to data portability (the transfer of data from one controller to another).

Profiling

Data controllers must inform data subjects of the existence and consequences of any profiling activities that they carry out (including online tracking and behavioural advertising).

Data protection by design

Organisations must apply the principles of data security by design and by default when developing new systems and services.

Standards

The GDPR encourages the adoption of international standards and certification.

Records

The Regulation places the onus on organisations to keep their own records of data processing activities and to make these available to the supervisory authority on request.

Accountability

Most healthcare organisations will be required to appoint a data protection officer (DPO) who will be responsible for monitoring compliance with the Regulation, providing information and advice, and liaising with the supervisory authority.

Notification

Organisations will have to report any data breach to the supervisory authority within 72 hours of becoming aware of it.

Penalty

The Information Commissioner's Office (ICO) will be able to impose maximum fines of up to 4% of annual global turnover or €20 million, whichever

Further information on the GDPR can be found in our compliance guide.

NIS Directive [iv]

The NIS Directive also comes into effect in May 2018 and EU member states have six months to define the critical services organisations to which it applies. Organisations operating in the healthcare sector have already been identified as potential operators of essential services (OES) that may need to comply with the Directive.

The UK government has published four overall objectives and, within these, 14 high-level security principles that all operators will be expected to comply with. These include:

Objective A

Appropriate organisational structures, policies and processes need to be in place to manage security risks. Organisations need to prioritise:

- **Governance:** Ensure appropriate management policies and processes are in place to govern the approach to the organisation's network and information security;
- **Risk management:** Take appropriate steps to identify, assess and understand security risks;
- **Asset management:** Understand all systems and infrastructure that are required to maintain operational functionality; and
- **Supply chain:** Manage security risks that arise from a dependency on an external supplier.

Objective B

Proportionate security measures must be in place to protect essential services and systems from cyber attack. This includes:

- **Service protection policies and processes:** Identify policies and processes to direct the approach to securing systems and data;
- **Identify and access control:** Controls must be in place granting access to systems and functions to appropriate users only;
- **Data security:** Prevent unauthorised access to data;
- **System security:** Protect network and information systems that are critical for the delivery of essential services from cyber attack;
- **Resilient networks and systems:** Build resilience to cyber attack by design into systems that support the delivery of essential services; and
- **Staff awareness and training:** Provide appropriate staff awareness and training to all employees to allow them to support the security of network and information systems.

Objective C

Ensure defences to detect cyber security threats remain effective. This includes:

- **Security monitoring:** Monitor the security status of network and information systems to detect potential vulnerabilities and track ongoing effectiveness; and
- **Anomaly detection:** Detect anomalous events in the network and information systems.

Objective D

Minimise the impact of cyber attacks to protect business continuity and restore service. This includes:

- **Response and recovery planning:** Put in place a defined and tested incident management process.
- **Improvements:** When breaches do occur, understand the cause and take appropriate remediating actions.

The NIS Directive also identifies:

International standards and NIS Directive compliance

The Directive requires member states to encourage the use of "European or internationally accepted standards and specifications relevant to the security of network and information systems".

The only relevant international standards against which organisations can achieve independently accredited certification are ISO 27001 and ISO 22301.accredited certification are ISO 27001 and ISO 22301.

Penalties for non-compliance

Member states must identify penalties for infringing the NIS Directive, and these must be "effective, proportionate and dissuasive".

Further information on the NIS Directive can be found in our green paper.

DSP Toolkit v

From April 2018, the DSP Toolkit will replace the IG Toolkit as the standard for cyber and data security for healthcare organisations. Compliance with the DSP Toolkit requires organisations to demonstrate that they are implementing the ten data security standards recommended by the National Data Guardian Review.

The DSP Toolkit is arranged into three categories of leadership obligations: people, processes and technology. These obligations include:

People

The DSP Toolkit requires that information security becomes a senior-level responsibility, with a named senior executive or board member responsible for cyber and data security, and that all staff receive the appropriate annual training related to data security and protection.

This leadership obligation also asks that all organisations complete the DoH checklist for GDPR compliance and remain compliant with the IG Toolkit v.14.1 until 31 March 2018.

Processes

To prevent and mitigate the effects of a data breach, the DSP Toolkit requires organisations to act on CareCERT advisories, report data security incidents in line with CareCERT reporting guidelines and put in place a "comprehensive business continuity plan" to respond to security incidents.

Technology

The DSP Toolkit requires technology to be effective in meeting cyber security needs.

This includes replacing unsupported systems as a matter of urgency; completing on-site cyber and data security assessments and acting on the results; and ensuring that any IT system provider holds the appropriate ISO 27001, Cyber Essentials or Digital Marketplace certification.

More information on the DSP Toolkit can be found on our information page.

Cyber resilience as a security and compliance tool.

There are a number of common principles across the GDPR, the NIS Directive and the DSP Toolkit. These include identifying and managing risks, implementing information security management best practices and developing a business continuity plan. Cyber resilience offers a solution to these common principles.

What is cyber resilience?

As cyber threats evolve, the rate of development of security solutions cannot always match the pace. Instead of focusing solely on preventing attackers from accessing your network, it is better to plan a strategy that reduces the impact of a breach if one does occur. Cyber resilience brings together cyber security and business continuity to help organisations protect against a breach, and to ensure your organisation's survival following an incident.

Cyber security

Cyber security consists of technologies, processes and measures that are designed to protect individuals and organisations from cyber crime. Effective cyber security planning involves identifying the threats and vulnerabilities facing the organisation and taking appropriate measures to mitigate those risks, balancing business objectives against the cost, impact and likelihood of those threats materialising.

A number of frameworks exist to help organisations reduce cyber risks. ISO 27001 is the international standard that describes best practice for an information security management system (ISMS) and is recommended to organisations planning and implementing cyber resilience strategies.

For more information on the range of behaviours, policies and processes addressed in ISO 27001, please see our green paper.

Business continuity management

Business continuity management involves the processes and procedures for the development, testing and maintenance of plans that will enable an organisation to continue operating during and after a disaster.

ISO 22301 sets out the requirements for a business continuity management system (BCMS) and is considered the only credible framework for effective business continuity management in the world.

For more information on the requirements set out in ISO 22301, please see our information page.

Their comprehensive approach to information security management and business continuity management means ISO 27001 and ISO 22301 are recommended as tools for complying with cyber and data security requirements and legislation.

Addressing common healthcare threats with cyber resilience

In the first section of this document, we identified common vulnerabilities facing healthcare organisations as identified in a combination of Verizon's 2017 Data Breach Investigations Report, the National Data Guardian Review and CQC's 'Safe data, Safe care'. Below we examine how ISO 22301 and various controls identified in ISO 27001 address these common cyber and information security threats.

THREAT/SOLUTION	CONTROL
Deliberate attack; hacking, malware and social	**ISO 27001 control**
Organisations should implement "detection, prevention and recovery" practices to protect against malware. This includes the management and segregation of networks and information processing facilities to protect information. Many practices are necessary to satisfy the broad topics of detection, prevention and recovery, and these are addressed across multiple controls.	A.12.2.1 / A.12.4.1 / A.12.6.1 / A.13.1 / A.16.1.2 / A.16.1.5 / A.17.1
To maintain the security of information as it is transferred outside of the organisation, policies, procedures and controls should be identified that address the use of all types of communication facilities. This includes the protection of information involved in electronic messaging and requirements for confidentiality and non-disclosure agreements.	A.13.2 / A.8.1.3 / A.8.3.3
Information on technical vulnerabilities should be obtained, evaluated and addressed in a timely manner to prevent the exploitation of technical vulnerabilities.	A.12.6
Secure coding should be accounted for to reduce the likelihood of cyber security incidents via web applications. This includes information security requirements being embedded in the design and development of new information systems or enhancements to existing systems, and the protection of information when passing over public networks.	A.14.1.1 / A.14.1.2 / A.14.2
Malicious insiders	**ISO 27001 control**
All candidates should be screened before employment relative to "business requirements, the classification of the information to be accessed and the perceived risks". This should highlight employees who might present a risk and allow for appropriate action to be taken to minimise this. This control also highlights that employees' terms and conditions should reflect responsible access and use of data, and these terms should continue after their employment termination, if appropriate.	A.7.1
Organisations should ensure restricted access to program source codes and utility programs that can override systems controls, and a log of user activity to record events and generate evidence of suspicious activity, respectively. This reduces the risk and scope of damage a malicious insider can cause and should allow for early detection of malicious behaviour.	A.9.4 / A.12.4 / A.9.1 / A.9.2
Unencrypted devices and non-anonymised data	**ISO 27001 control**
To minimise the impact of devices being lost or stolen, organisations must identify all assets associated with information and information processing facilities, and should define policies for the acceptable use and return of these assets. Information available on devices should be assigned an appropriate classification and an equivalent level of protection, and policies should be identified and communicated for the correct use, modification or disposal of information stored on devices.	A.8.1 / A.8.2 / A.8.3
Organisations should identify a policy on the use of "cryptographic controls for protection of Information" to prevent the use or compromise of unencrypted devices. The Standard includes nine controls on the preventions of loss, damage, theft or compromise of assets to comprehensively secure data from a variety of threats affecting mobile devices.	A.10.1

Employee behaviour	ISO 27001 control
ISO 27001 recommends "management direction and support" for information security. This includes the development and communication of policies to all relevant employees and external parties. Ensuring that information security is seen as a management objective increases the gravitas placed upon it by all employees of the organisation.	A.5.1
All employees and relevant contractors should receive "appropriate awareness education and training" and regular updates on policies and procedures. This control also states that a formal and communicated disciplinary process should be in place against employees who cause an information security breach.	A.7.2
To minimise the risk of unauthorised access, organisations should adopt secure log-on procedures and policies relating to password management and the use of quality passwords. Access privileges to networks and services should also reflect the remit of the employees' role to reduce company-wide access to sensitive systems.	A.9.4 / A.9.1 / A.9.2
To ensure the integrity of operational systems, procedures need to be implemented to "control the installation of software on operational systems". This should notify organisations of any technical 'workarounds' that staff have implemented and allow appropriate security measures to take place to mitigate against these.	A.12.5.1
Business continuity	**Standard/control**
ISO 22301 is the international standard for business continuity management. It identifies processes to help an organisation comprehensively understand its needs, plan for business continuity in the event of a breach, ensure business continuity planning is a management commitment and evaluate performance for continual improvement.	ISO 22301
Information security continuity should be embedded in business continuity management. Organisations should determine requirements for information security and the continuity of the ISMS in adverse situations. Organisations should implement processes, procedures and controls necessary to ensure information security continuity and this should be reviewed regularly.	ISO 27001 control A.17.1

Implementing an integrated management system that comprises an ISMS and BCMS will give your organisation an internationally accepted posture of cyber resilience based on risk management best practice – exactly as the new legislation requires – as well as removing the burden of multiple compliance audits.

IT Governance products and services
ISO 27001

IT Governance is globally known as the authority on ISO 27001. Our team successfully led the world's first ISO 27001 certification project and we have worked for the past 15 years to hone our wide range of tools and solutions, including toolkits, training, standards, software and consultancy.

Bringing together the range of products available, our DIY packages offer the most comprehensive mix of ISO 27001 tools and resources on the market to meet the unique needs of an organisation. Discover a tailored approach to certification with one of our four expertly curated packages.

More information on ISO 27001 solutions

ISO 22301

Effective business continuity management means an organisation can resume operations and return to 'business as usual' as quickly as possible after a disruptive incident, such as a cyber attack or power failure.

An ISO 22301-aligned BCMS will include disaster recovery plans, which focus on the recovery of specific operations, functions, sites, services or applications.

More information on ISO 22301 solutions

The GDPR

Our GDPR experts can help your organisation with a variety of best-practice solutions, from evaluating your GDPR compliance position and developing a remediation roadmap, through to implementing a best-fit data compliance framework.

Training is key to achieving best practice in data protection and information security. IT Governance's certified Foundation and Practitioner training courses equip attendees with the specialist knowledge and skills needed to deliver GDPR compliance.

For organisations looking to bring in market-leading data protection knowledge, DPO as a service is available. This involves one of our dedicated experts taking responsibility for the function of the DPO, allowing you to stay focused on your core business activities.

For more information on the requirements of the GDPR and to discover how IT Governance can help you achieve compliance and improve security, please visit our website.

More information on GDPR solutions

IG Toolkit

Until 31 March 2018, compliance with the IG Toolkit v.14.1 is obligatory for healthcare organisations.

IT Governance can assess your organisation's current level of compliance against the 2017–18 standards, develop your IG Toolkit improvement plan for the first time or provide ongoing support to help facilitate continuous compliance with the requirements of the IG Toolkit, on time and within budget.

From April 2018, the DSP Toolkit will replace the IG Toolkit. More information on the DSP Toolkit can be found on our information page.

For more information on the range of services we offer healthcare organisations, talk to one of our experts.

Technical services

Healthcare organisations may have the technology and procedures in place to prevent data theft, but it's difficult to find every security weakness.

To help protect your network and electronic patient health information, you need to examine your environment the way a potential attacker would. Penetration testing is essentially a controlled form of hacking in which the 'attackers' operate on your behalf to find the sorts of weaknesses that criminals exploit.

IT Governance is a CREST member company, meaning that clients can rest assured that our penetration tests will be carried out to the highest standards by qualified and knowledgeable individuals.

More information about security testing

i. www.verizonenterprise.com/verizon-insights-lab/dbir/2017/.

ii. www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF.

iii. www.cqc.org.uk/sites/default/files/20160701%20Data%20security%20review%20FINAL%20for%20web.pdf.

iv. Information derived from the NIS Directive: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

v. Information derived from the 2017–18 Data Security and Protection Requirements: www.gov.uk/government/uploads/system/uploads/attachment_data/file/655876/171027_2017-18_Data_Security_Requirements.pdf.

IT Governance Ltd

Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park, Ely,
Cambs. CB7 4EA. United Kingdom.

t: +44 (0)333 800 7000
e: servicecentre@itgovernance.co.uk
w: www.itgovernance.co.uk

/ITGovernanceLtd /ITGovernanceLtd /ITGovernanceLtd