The WannaCry Attack: An Evaluation of Centrally Mandated Information Governance for the English NHS and Local Government

Tony Leary

Technical Report

RHUL–ISG–2020–5

22 June 2020

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Student Number: 100886647

Anthony Leary

THE WANNACRY ATTACK: AN EVALUATION OF CENTRALLY MANDATED INFORMATION GOVERNANCE FOR THE ENGLISH NHS AND LOCAL GOVERNMENT

Supervisor: Geraint Price

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date: 21st August 2019

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Page Intentionally Left Blank

Keywords

NHS, WannaCry, Ransomware, Security Management, Local Government, Local Authorities, Health and Social Care Information Centre, HSCIC, NHS Digital, information governance, cyber security, malware, information security.

Acknowledgements

I would like to express my gratitude to my course advisor, Prof. Peter Komisarczuk, and my project supervisor, Dr Geraint Price, for their guidance.

And a huge thank you to Sara, my wife, and to my children, Danny and Erin. Their support and understanding over the last two years allowed me to focus, not only on this project, but the whole MSc programme.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ANM	Advanced Network Monitoring [within HSCN]
CE	Cyber Essentials
CE+	Cyber Essentials Plus
CIA	Confidentiality, Integrity and Availability
CoCo	Code of Connection
CVSS	Common Vulnerability Scoring System
DPA	[UK] Data Protection Act (1998 or 2018)
DSPT	Data Security Protection Toolkit
EU	European Union
FOI	Freedom of information
FOIA	[UK] Freedom of Information Act (2000)
GCHQ	[UK] Government Communications Headquarters
GDPR	[EU] General Data Protection Regulation
GDS	[UK] Government Digital Service
HSCIC	Health and Social Care Information Centre (NHS)
HSCN	Health and Social Care Network
ICO	[UK] Information Commissioner's Office
IEC	International Electrotechnical Commission
IGT	Information Governance Toolkit
ISO	International Organization for Standardization
ISO 27001	ISO/IEC 27001:2013
ISO 27002	ISO/IEC 27002:2013
ITHC	IT Health Check
LA	[UK] Local Authority
N3	New NHS Network
NAS	Network Analytics Service [within HSCN]
NCSC	[UK] National Cyber Security Centre
NHS	[UK] National Health Service
NIST	[US] National Institute of Standards and Technology
NSA	[US] National Security Agency
NVD	[US] National Vulnerability Database
PAC	[UK] Parliamentary Accounts Committee
PERC	Privacy and Electronic Communications (EC Directive) Regulations 2003
PSN	Public Sector Network
RHUL	Royal Holloway, University of London

Executive Summary

In May 2017, a strain of ransomware called ‘WannaCry’ infected 32 National Health Service (NHS) trusts in England. It was able to self-replicate and spread via data networks, including the NHS national data network (N3). The NHS’s report on the incident noted that all English local authorities (LAs) reported being unaffected, despite also being connected to N3. Neither the NHS report nor the subsequent UK Parliament report sought to explain why LAs avoided infection. This project aims to answer that question by evaluating the relative strengths and weaknesses of the centralised security governance systems in place for NHS trusts and local government organisations, both before and after the WannaCry attack. Publicly available data on historical security breaches for NHS trusts and LAs are also analysed for patterns of security control failure that may indicate NHS trusts were at a higher risk of infection. The application of a standard information security control set, ISO/IEC 27002:2013, enabled the different information governance systems and security breach reporting data to be more easily compared.

The results indicated that the NHS’s centralised governance in place at the time of the WannaCry attack was weaker than the equivalent governance applying to local authorities. The changes in NHS governance since the WannaCry attack address these weaknesses, while implicitly confirming their existence. The security breach data revealed no significant variation in the root cause control failures for either the NHS or LAs; however, the variation in data focus and quality limits this project’s confidence in stating this authoritatively. It is recommended that the UK government standardise its security breach reporting to ensure that root cause data is consistently recorded, allowing standard security controls definitions, such as ISO/IEC 27002:2013 Annex A to be more easily applied to breach data. A standard data set could highlight areas of strength, or weakness, in information governance across government; guidance can then adapt accordingly.

Chapter 1: Introduction

1.1 CONTEXT

Between the 12th and 15th May 2017, the UK National Health Service (NHS) was the victim of a widely reported malware infection that crippled parts of the organisation. It led to the cancellation of some patient services, including operations [1]. NHS England subsequently released a report “Lessons learned review of the WannaCry Ransomware Cyber Attack” [2]. The report included the following observation:

“Based on a 100% return from local authorities to COBRA [the UK government emergency response committee] in the aftermath of WannaCry, no local authorities reported having been infected” [2, p. 14].

The NHS England report does not explore the reason for this apparent disparity between two sets of organisations that share many similarities; being broadly autonomous (politically in the case of local authorities), numerous (343 local authorities [3] and 152 NHS hospital trusts in England) [4] and geographically diverse. NHS trusts and local authorities (LAs) were also interconnected via a shared data network called ‘N3’ [5] that was the source of infection for some NHS organisations [6, p. 11].

1.2 OBJECTIVES

The primary objective of this project is to seek to explain why the NHS was adversely impacted by the WannaCry attack when local authorities were not. The following sub-objectives were selected to support achieving the project’s objective.

1. Sub-objective: Provide an overview of ransomware.
2. Sub-objective: Provide an overview of WannaCry. Classification and analysis of information security control failures necessary for the WannaCry attack to succeed, using ISO/IEC 27002:2013 controls.

3. Sub-objective: Classification and analysis of NHS England’s centrally mandated information security controls in place at the time of the WannaCry attack using ISO/IEC 27002:2013.
4. Sub-objective: Classification and analysis of the UK Cabinet Office centrally mandated information security controls in place at the time of the WannaCry attack using ISO/IEC 27002:2013.
5. Sub-objective: Analysis of publically available information security breach data for NHS trusts and local authorities in England, classifying root causes with applicable ISO/IEC 27002:2013 controls.
6. Sub-objective: Concluding analysis, evaluation, observations and, potentially, recommendations.

1.3 STRUCTURE OF THE REMAINDER OF THIS DISSERTATION

This project is organised into five further chapters. Each chapter within this project includes, where relevant, the source and search rationale for its underpinning literature review.

The RHUL LibrarySearch service is the primary source of the academic literature that informs this project. Where grey literature was used, priority was given to sources that are generally accepted as neutral, as well as being easy to access, e.g. free of login requirements, such as the BBC.

Chapter 2 Background

This chapter provides the reader with contextual information on the key technologies and organisations covered within this project. Ransomware is explained first, as a primer to an overview of the WannaCry attack. The structure of the NHS and LAs and how they are linked is also described. Finally, three UK government reports, from the National Audit Office, NHS and UK parliament, are analysed to establish the root causes of the WannaCry attack.

Chapter 3 Governance review

This chapter introduces the ISO/IEC 27001:2013 standard (ISO 27001) and the ISO/IEC 27002:2013 code of practice (ISO 27002). The root cause analysis of the WannaCry attack from chapter 2 is used to evaluate the security controls that would be applicable, based on ISO 27001 Annex A, that summarises the ISO 27002 controls.

The primary data sources for centrally mandated information governance controls are websites relevant to the NHS and local government. Breach data was gathered from the NHS and information commissioner's office websites. The root cause analysis for the WannaCry attack is then evaluated in turn against the centralised information governance schemes in place for the NHS and LAs both before, and after, the WannaCry attack.

Chapter 4 Data collection methodology

Various sources of security incident and breach data for the NHS and LAs are discussed, and their output evaluated. Suitable data are identified for analysis in chapter 5, with a focus on data that allows for a determination of the root cause of the incident or breach, so enabling the evaluation of the applicable control set(s) from ISO 27001 Annex A in chapter 5. A further pre-requisite of the data is that it allows both the NHS and LAs to be compared within the same period.

Chapter 5 Data analysis

A subset of the data evaluated in chapter 4 was carried over into this chapter for detailed analysis. ISO 27002 controls provided a consistent framework for the analysis of the controls in place for the NHS and local government, as well as of the control failures determined to be the root causes within the collected breach data. Information security governance may rely on multiple, overlapping controls, so the analysis established the 'primary' and 'secondary' controls; either in place or judged to have failed.

This project is focused on the root cause of breaches since cases can have similar 'symptoms' but have different root causes. For example, the root cause of the loss of an unencrypted USB stick containing personal data may be the failure to have a policy in the first place ("A.8.3.1 handling of removable media" [7, p. 12]), or perhaps a policy existed, but it was not communicated adequately to staff ("A.7.2.2 information security education, awareness and training" [7, p. 11]). The data sets were therefore aggregated where necessary and filtered, leaving only the relevant NHS and LA data that was sufficiently detailed to allow an evaluation of the failing security ISO 27001 Annex A control(s). The various steps undertaken to cleanse the data are documented and the results provided in tables both within the chapter and as appendices; diagrams also provide summaries of the data evaluation undertaken.

Chapter 6 Conclusion

This project concludes with a summary of the findings from chapter 3 governance review and chapter 5 data analysis. The limitations encountered are also described. Finally, recommendations are offered.

Chapter 2: Background

2.1 APPROACH

Descriptions of ransomware, the WannaCry attack, the NHS in England and local government in England all provide context to the later analysis and discussions within this project. Authoritative UK government reports on the WannaCry attack are reviewed, with a focus on discovering the root causes.

2.2 WHAT IS RANSOMWARE?

2.2.1 Literature search methodology:

1. Use RHUL LibrarySearch: search terms "Ransomware AND Malware."
2. Undertake a general Google search for other authoritative sources, such as IT security vendors and news sites.

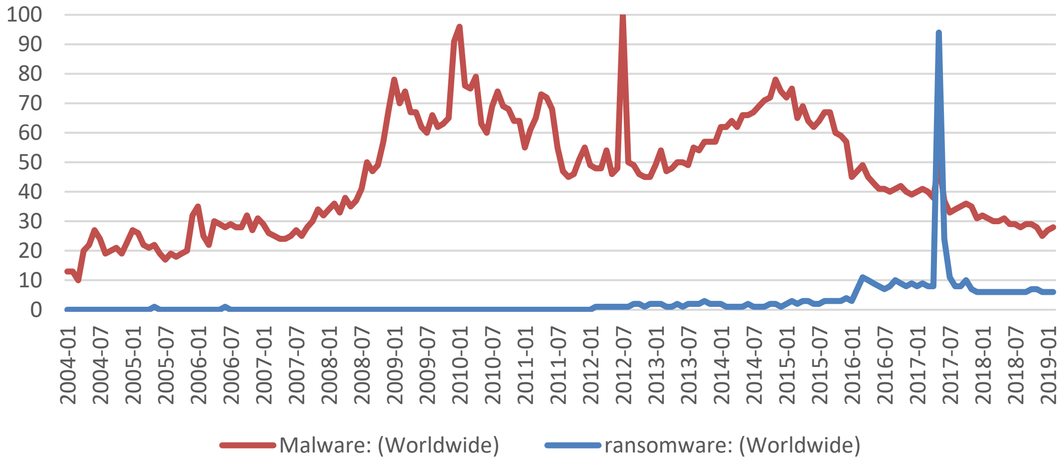
This section will review the literature available regarding ransomware before the WannaCry outbreak that affected the NHS from 12th May 2017 [6, p. 4] The reason for limiting the literature review in this way is due to the attack's significance as a 'signal moment' [8] (derived from the concept of a 'signal crime' [9]) that accordingly generated an enormous amount of press and academic comment. Therefore, constraining the review to before the attack allows this section to focus on the predictability, or otherwise, of such an event within the NHS. The WannaCry attack itself is also the subject of a discrete section within this project and includes a literature review. A Wikipedia article on ransomware defines it thus:

"Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid" [10].

A Google Trends search was run [11] to compare the relative, worldwide frequency of the search terms "ransomware" and "malware" from Jan 2004 (the earliest available) to 18th Feb 2019. The Figure 1 Google search term trends: malware & ransomware 2004 to 2018 chart (Figure 1), while not an academically authoritative source for popularity of terms in use, shows that despite its effective creation in 1996, ransomware was, relative to the July 2017 peak, barely searched for until 2012, whereas malware is a term that has been searched for throughout the period shown.

Searches for ‘ransomware’ slowly increase until a spike in May 2017 that coincided with the WannaCry outbreak.

Figure 1 Google search term trends: malware & ransomware 2004 to 2018 [11]



Note that a Google Trends search that included ‘cryptovirology’ registered very few searches over the period, relative to ‘ransomware’, so was omitted from the graph for the sake of clarity.

An initial literature search using RHUL LibrarySearch [12] was conducted with the search term “Ransomware” and then filtered for only peer-reviewed articles, returning 564. Filtering items dated up to and including 11th May 2017, which deliberately excludes the NHS WannaCry outbreak, returned 234 results. A further filter “NOT WannaCry” was applied to the search to remove any WannaCry references that remained, the results further reduced to 218 [13]. From an initial review, some foreign language articles appeared, so the search was further refined to include English-only results, leaving 200 articles. Reviewing and filtering left 122 results [14]. This project is not undertaking a detailed analysis of ransomware, so articles covering specific technical aspects of ransomware such as detection and mitigation were removed, A more in-depth review of the article subjects resulted in 83 items.

The 83 items were all read and reviewed for relevance to this section. These were a mix of research papers and journal articles.

2.2.2 History of ransomware

Malicious software, more commonly referred to by the portmanteau ‘malware’, can be traced back to the 1970s [15]. Ransomware is a newer, sub-type of malware whereby an attacker will seek to extort money from a victim by denying them access to their data and then charging a fee to restore that access.

As a form of extortion, ransomware is a ‘cyber-enabled’ crime. Computer crime is commonly classified as either ‘cyber-enabled’ or ‘cyber-dependent’ [16, p. 5]. Cyber-enabled crimes are ‘traditional’ crimes that are amplified by the computational power of computers, or the greater (potentially global) reach of computer networks such as the internet [16, p. 5]. Conversely, cyber-dependent crimes would not exist, but for the invention and availability of computers and computers networks [16, p. 5]. If malware aimed to deny the victim access to their data, with no opportunity to pay to restore access, this ‘denial-of-service’ would be a cyber-dependent crime.

The first example of ransomware was the AIDS trojan, created in 1989 by an AIDS researcher who posted infected floppy disks to the 20,000 attendees of an AIDS conference [17]. The malware encrypted the file names of the victims’ hard disk drive and demanded payment by cheque to a Panama-registered company. A UK virus researcher developed a program to remove the AIDS trojan and described the encryption used as “fairly simple” [17, p. 6].

The sophisticated ransomware that is the subject of this project has its genesis in a 1996 research paper “Cryptovirology: Extortion-Based Security Threats and Countermeasures” [18, p. 129]. The authors explored the “offensive” use of cryptography for extortion, or denial-of-service, even going so far as to compare the potential for the ‘weaponisation’ of cryptography to nuclear fission [19, p. 53]. They refer back to the AIDS trojan as an example of the ideal “symbiotic relationship” that they were seeking to emulate, where the victim ‘host’ cannot remove the malware without harming its data [18, p. 131]. The paper also describes a proof of concept “*crypto virus*” developed to deliver an encrypting payload that utilises ‘hybrid cryptography’: a system comprising both public-key and symmetric-key cryptography. The authors offered mitigations, including the need to protect any cryptographic software libraries available for use, to reduce the risk of an attacker using them maliciously. The paper was prescient, as modern Microsoft Windows ransomware variants, including WannaCry, use the techniques described, including the use of the pre-installed cryptographic software library included in Microsoft Windows, and hybrid encryption [20].

A ransomware attack was explicitly reported in the 'IEEE News Brief' July 2005 article titled "Unusual attack holds computer files for ransom" [21, p. 25]. It goes on to describe the attacker wanting "$200 via e-gold—an e-payment company" and that it "…appears to be a proof-of-concept attack." Also noteworthy is that the strong hybrid encryption proposed by Young and Yung [18, p. 129] was not used. The attack instead relied on "weak obfuscation", and although the ransom was not paid, contributors speculated that if it was, "Investigators could follow the money trail" [21, p. 25].

The traceability of a ransom payment is a significant risk to the perpetrator, hence the common crime fiction trope of ransom demands paid in 'unmarked bills'. Banknotes have a unique serial number, so are potentially traceable. Ransoms may, therefore, be requested in 'non-sequential' notes, on the perhaps optimistic basis that a contiguous series of notes would be recorded, whereas non-sequential notes would not be. When this 'traditional' ransom scenario is applied to cyberspace, where attacks may affect thousands of victims, the assumption must be that ransoms will be paid electronically. However, given the pervasive, global regulation of electronic finance, this will, in all likelihood, lead to a 'money trail'.

2.2.3 The growth of ransomware

The electronic equivalent of 'unmarked bills' arrived in 2008, with the creation of the Bitcoin cryptocurrency in 2008 [22]. Bitcoin is a virtual, computer-based currency that provides transactional and storage security, as well as a degree of anonymity as there is no requirement for a user's identity to be established authoritatively [19, p. 562]. This is a feature Bitcoin shares with traditional fiat currencies such as the British pound sterling and US dollar.

Cryptocurrencies such as Bitcoin can allow users to remain anonymous despite all transactions being visible in the 'blockchain' ledger that records both the transactions and the participants included in those transactions [19, p. 562]. However, this anonymity is only maintained while a user's currency remains within the cryptocurrency system. A user may decide to convert their 'crypto coins' into a conventional currency such as US dollars and organisations exist to provide exchange services for cryptocurrencies, analogous to conventional currency exchanges that would, for example, convert pounds sterling to US dollars for a fee. As such, an entity wishing to exchange Bitcoin for US dollars will transfer Bitcoin value to the exchange, which will also be a user within the same cryptocurrency system, resulting in a record of the transaction in the blockchain. On receipt of the cryptocurrency, the exchange will pay the seller the agreed value in their chosen currency. Assuming the exchange is law-abiding, the payment in any conventional currency is highly likely to be in the form of an electronic transfer. At this point, an audit trail is created from the 'real world' back into the cryptocurrency system, potentially linking the user's 'real' identity to all their previously anonymous transactions. Hence, for a criminal wanting to convert cryptocurrency, this creates the risk of being identified and perhaps arrested [23, p. 21].

Some vendors accept Bitcoin, so the possibility of using Bitcoin 'conventionally' as a direct means of exchange does exist, though buying goods or services from law-abiding vendors, such as Microsoft [24], will again risk the creation of an audit trail. Cryptocurrencies could be considered a catalyst for cybercrimes such as ransomware since they "…make it as easy as possible to pay the ransom" [23, p. 22].

Although ransomware was effectively invented in 1996, the Google Trends graph (Figure 1) implies a low public awareness of ransomware until 2012, then a slight increase until the spike that coincides with the 12th May 2017 WannaCry event.

In September 2013, a new strain of ransomware called 'Cryptolocker' was discovered, which led to thousands of infected devices [25]. An extensive analysis in 2014 [26], used the public nature of Bitcoin transactions to trace and track Bitcoin addresses used by Cryptolocker. The ransom was $300 initially but varied due to the attackers providing two options for payment: MoneyPak, a US electronic payment company or; Bitcoin, the value of which varied substantially over the research period [26, p. 3]. Between September 2013 to January 2014, the paper estimates "795 ransom payments" totalling at least "$310,472.38" [26, p. 1]. It is clear that ransom figures vary: the reported 'ransom' to unlock an affected device in 2015 ranged from $100 to $500 [27, p. 82]. There is also an example of security vendor researchers merely asking for, and receiving, the master key [28], albeit after "the perpetrators extorted $76,522 from 163 victims" [29].

The scale of attacks suggests that substantial IT infrastructure is required to distribute and then manage ransomware campaigns. The 2012 "Threat Landscape" report [30] from the European agency for cybersecurity (ENISA) describes botnets as:

"…multiple usage tools that can be used for spamming and identity theft as well as for infecting other systems and [distributing] malware" [30, p. 16]. Moreover, that: "…botnets are used as a commodity. Interested parties can rent botnet in order to achieve their purposes" [30, p. 16]. This commoditisation of the 'criminal computing' that botnets provide has also earned the moniker "Malware-as-a-service" [31, p. 192].

The availability of botnets for hire and the potential anonymity offered by cryptocurrencies, provide cybercriminals with both the 'means' and 'motive' to carry out cybercrime, leaving only the discovery of their 'opportunity.

2.2.4 Operation of ransomware

Like all malware, ransomware does not exist on computing devices 'by default': that is to say, it is not a feature in an infected device's original programming code. What malware will often do, however, is exploit vulnerabilities in that original code, though there have also been instances of vendors shipping devices that inadvertently included malware [32]. This is the 'opportunity' malicious entities, such as a cybercriminal, must discover. A practical example would be a malware infection occurring through users merely accessing websites where a 3rd party advertising provider had served infected adverts to 'innocent' websites [33, p. 16].

The plethora of attack options available to a malicious entity necessarily results in defenders adopting security controls that seek to mitigate the threats. Defence in depth is a military term analogous to the approach taken to protect information systems from attack: multiple, overlapping controls all act to reduce the risk of an attack to the level an organisation can accept. Controls can focus on the human aspects of information security, such as written policies and awareness training, as well as the technical aspects, e.g. anti-malware software, firewalls and intrusion prevention systems. Failure should also be planned for, and a US Federal Bureau of Investigation report in 2015 highlighted the importance of being able to recover effectively from denial-of-service, that is at the heart of a ransomware attack, through "…creation of a solid business continuity plan" [34]. The need to defend, as well as preparing to recover from an attack, is a common theme [35, p. 23], [36, p. 30].

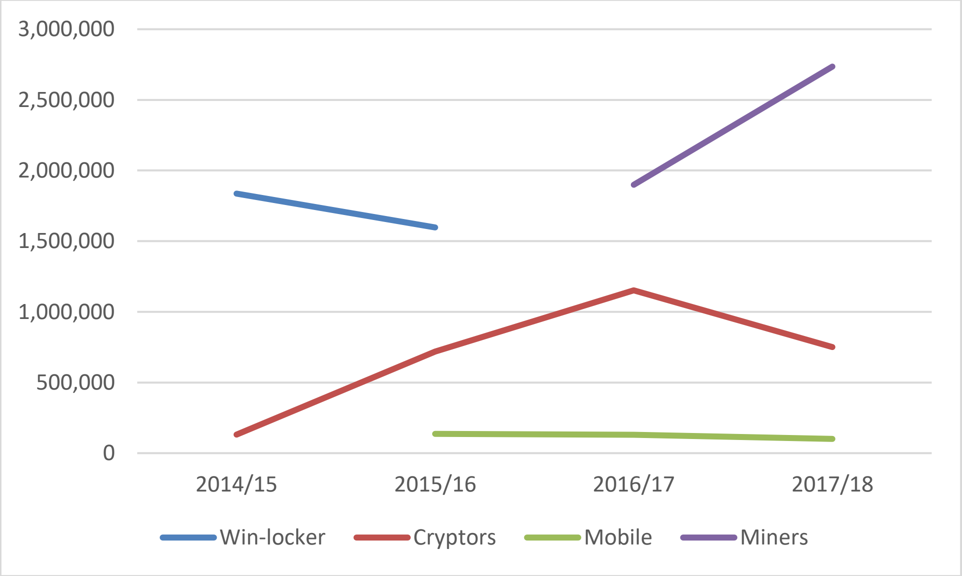
2.2.5 The future of ransomware

The security vendor Kaspersky Labs investigated ransomware infections experienced globally by its customers through a series of reports [37]–[39] that tracked four ransomware categories. These are defined as:

- *Win-locker*: A ransomware variant that locks system components preventing their use.
- *Cryptors*: Encrypting ransomware, in the style of WannaCry et al.
- *Mobile*: A ransomware variant running on a mobile device.
- *Miners*: Malware that remains hidden in order to steal system resources for cryptocurrency mining. There is no ransom demanded, so this is not ransomware per se.

The ransomware volume data within the reports were used to create the Figure 2 graph.

Figure 2 Kaspersky ransomware detection trends [37]–[39]



The growth in cryptors, such as WannaCry, can be seen in Figure 2; from 2014/15, up to a peak in 2016/17. It is notable that the appearance and volume of mining malware substantially exceeded the 2016/17 peak in cryptors, without generating as much press attention. One conclusion is that the publicity associated with large scale ransomware, such as WannaCry, led to an increase in operating risk for ransomware attackers. Some may have chosen to give up their “ideal symbiotic relationship" [18, p. 131] for the longer term 'parasitic' approach of cryptocurrency mining, that is much less high profile and so perhaps, lower risk.

In June 2017, Young and Yung [40] reflected on the impact of ransomware in an article titled "Cryptovirology: the birth, neglect, and explosion of ransomware". After their 1996 work that combined publicly available cryptography and malware into what subsequently became ransomware, they were critical of the IT security community's failure to prevent its rise. Later in 2017, they blame the lack of progress in tackling ransomware on a research gap in cryptovirology caused, in part, by "group conformity" among security researchers [41, pp. 83–84].

Other research examines the potential for ransomware to impact devices beyond those laptop, servers and mobile devices known to be at risk. Examples detail incidences affecting a Smart TV and a proof-of-concept attack on smart bulbs [42, p. 447]. This demonstrates that even the unconventional computing devices, that contribute to the 'Internet of Things', are not immune to the threat of malware.

In conclusion, organisations must rely on defence-in-depth to avoid a ransomware infection; prompt patching, anti-malware controls, strong access controls and effective boundary protections, are likely to prevent the majority of attacks. However, data backups provide a 'safety net' in the event that the other technical security controls fail, so are an essential component of any organisation's defence.

2.3 THE WANNACRY ATTACK

2.3.1 Literature search methodology:

1. Review UK government published reports on the WannaCry attack.
2. Review 66 peer-reviewed articles returned from LibrarySearch text "WannaCry And Cause" focusing on those that analyse rather than report the event.
3. Review vendor material (Microsoft) for information.
4. Review security vendor material for industry insights.

The top three results from the search are authoritative UK Government sources. In order of publication, these were the National Audit Office (24th October 2017) [6], the NHS (1st February 2018) [2] and the UK Parliament Public Accounts Committee (18th April 2018) [43].

Methodology: Search in RHUL LibrarySearch: “WannaCry And Cause”. Filtered for peer-reviewed articles and security, computing subjects. The search returned 38 results [44].

The WannaCry ransomware attack was widely reported due to its global reach and highly public impact on the NHS [45]. Accordingly, it is a commonly occurring example in the literature [41, p. 82], [46, p. 11]. WannaCry included code that originated from an exploit tool called ‘EternalBlue’ [47] that was among a more extensive suite of exploits stolen from the US National Security Agency (NSA) by a hacker group known as ‘Shadow Brokers’ [48]. WannaCry demanded its ransom in Bitcoin and researchers were able to monitor the three accounts used (known as ‘wallet addresses’) and detect the extraction of funds raised by the ransomware campaign. £108,953 in Bitcoin was withdrawn from the wallets during July and August 2017 [49].

Only one paper [48] reviewed provided a comprehensive technical summary of the events surrounding the WannaCry attack, such as the theft of the underlying exploit from the NSA and its subsequent release onto the internet. It also examined the probable availability of vulnerable servers on the internet that could be found and remotely exploited. The paper was published on 15th May 2017, only days after the attack began and three days before the NHS closed their major incident for the attack. It is therefore understandable that the author overemphasised Windows XP as the root cause of the NHS’ particular vulnerability, when in fact the subsequent UK National Audit Office (NAO) report [6] stated that most affected units were unpatched Windows 7 devices [6, p. 18].

The WannaCry attack was halted on the evening of the 12th May 2017 by a UK security researcher who, after analysing the network traffic from a WannaCry infected device, saw messages to a non-existent internet website. He registered the website name and his test sample of WannaCry no longer activated, allowing him to confirm it was disabled [50]. Also noteworthy was WannaCry’s ability to self-replicate [51, p. 29], potentially allowing an infected internet-facing server to act as a ‘bridgehead’ into the internal network, bypassing any firewall in place that did not have an intrusion prevention service.

The discovery and activation of the kill-switch that halted WannaCry is a weakness that its author had presumably thought unlikely. However, techniques for halting, or entirely removing ransomware are not unusual. Ransomware authors are human and may make coding errors that allow security researchers to create a 'decryptor' [51, p. 29] countermeasure that removes the ransomware, restoring the victim's files [52]. Other researchers have proposed methods to add coding to storage files to make decrypting ransomware easier. Example include the exploitation of the weaknesses inherent in the ECB and CBC modes of operation for block encryption [53, pp. 9–10], and the monitoring of device file system activity for a large number of changes that may indicate that ransomware is encrypting storage [54, pp. 15–17]. It is notable that these countermeasures do not include better protection of the cryptographic library exploited by ransomware, which was proposed by Young and Yung in 1996 [40, p. 137].

The presence of unpatched vulnerabilities on interfacing-facing NHS systems perhaps made some form of malicious exploitation highly likely. The self-replication used by WannaCry may have allowed the attack to spread laterally within NHS trusts and then onward to other trusts through any poorly protected boundary links, e.g. the internet and N3.

2.3.2 The WannaCry attack: vulnerability reporting

The global resource for IT vulnerability data is the National Vulnerability Database (NVD), a service provided by the US National Institute of Standards and Technology (NIST) [55]. Vulnerabilities submitted to the NVD are classified by the submitters (typically software vendors) according to the Common Vulnerability Scoring System (CVSS) [56]. It is a sophisticated methodology that uses multiple factors to calculate an overall 'base score' between zero and ten for a vulnerability [57]. One of five optional severity labels can also be applied, depending on the base score.

Table 1 CVSS 3.0 severity scale from [58, Sec. 5]

CVSS 3.0 Severity	**CVSS 3.0 Base Score**
None	0.0
Low	0.1-3.9
Medium	4.0-6.9

CVSS 3.0 Severity	CVSS 3.0 Base Score
High	7.0-8.9
Critical	9.0-10.0

Table 1 shows the five severity levels for vulnerabilities. There is a distinct narrowing of the range of values as the severity increases, which is designed to help organisations focus on the most severe vulnerabilities, hence ‘critical’ (a quarter of the available labels for severities greater than zero) applies to only a tenth of the possible base scores. Would the attack have succeeded if only ‘critical patches’ had been applied?

The WannaCry attack relied on specific Microsoft Windows vulnerabilities [6, p. 18] that were published by Microsoft within a ‘critical’ security bulletin called ‘MS 17-010’ on 14th March 2017 [59]. Microsoft submitted the five underlying vulnerabilities to the industry NVD on 16th March 2017, each with a CVSS base score of 8.1, equating to a severity rating of ‘high’ [60]–[64]. This rating was obviously at odds with Microsoft’s previously published rating of ‘critical’, so a review of the NVD vulnerability submission process was undertaken to investigate this discrepancy.

Each NVD vulnerability assessment includes the underlying metrics used to determine the base score. Table 2 CVSS 3.0 metrics and values, based on [58, Secs 6 and 8.4] summarises the components of a CVSS 3.0 score and the values assigned to each metric.

Table 2 CVSS 3.0 metrics and values, based on [58, Secs 6 and 8.4]

Metric	Metric Value	Numerical Value
Base Scores (Mandatory)		
Attack Vector	Network	0.85
	Adjacent Network	0.62
	Local	0.55
	Physical	0.2
Attack Complexity	Low	0.77
	High	0.44
Privilege Required	None	0.85
	Low	0.62 or 0.68
	High	0.27 or 0.50

Metric	Metric Value	Numerical Value
User Interaction	None	0.85
	Required	0.62
CIA Impact	C (High, Low, None)	0.56, 0.22, 0
	I (High, Low, None)	0.56, 0.22, 0
	A (High, Low, None)	0.56, 0.22, 0
Temporal Scores (Optional)		
Exploit Code Maturity	Not Defined	1
	High	1
	Functional	0.97
	Proof of Concept	0.94
	Unproven	0.91
Remediation Level	Not Defined	1
	Unavailable	1
	Workaround	0.97
	Temporary Fix	0.96
	Official Fix	0.95
Report Confidence	Not Defined	1
	Confirmed	1
	Reasonable	0.96
	Unknown	0.92
Environmental Scores (Optional)		
Modification of all Base Scores	As per Base Scores	As per Base Scores
Security Requirements CIA	Not Defined	1
	High	1.5
	Medium	1
	Low	0.5

Table 2 shows the three sections that make up a CVSS 3.0 base score. Only the first section, “Base Score Metrics”, is mandatory and is, therefore, the only section that must be completed to generate a CVSS base score. The equations used to calculate the base score go beyond the simple addition of the values shown in Table 2. For example, the resulting values from the first four base score metrics in Table 2 are multiplied together, and with ‘8.22’, and then added to the result of another formula that includes the “CIA Impact” values [58, Sec. 8.1].

All five vulnerabilities relating to MS 17-010 have the same base score, so one, ‘2017-143, was chosen for analysis within the on-line CVSS 3.0 calculator [65]; only base score metrics section had been completed. The remaining two sections, “Temporal Score Metrics” and “Environmental Score Metrics”, therefore, had no impact on the overall base score. To evaluate the effect of these two optional sections, the online CVSS calculator [66] was used to update the temporal section for 2017-143 based on there being a highly automated exploit available (which was undoubtedly the case on 12th May 2017), but mitigated by the availability of an official patch. Adding these resulted in the base score decreasing, from 8.1 to 7.7. This was determined to be due to the "Official Fix" entry for "Remediation Level", which multiples the other values by 0.95. The "Exploit Code" and "Maturity Report Confidence" metrics are '1' for both the highest-rated metric value for each, and "Not Defined" (see Table 2), which meant that selecting these had no overall effect on the base score.

Values for the environmental section were copied from the 'base' section, however doing this had no effect on the base score; the purpose of the environment section is to apply modifiers based on local circumstances, e.g. 'real' data is of low confidentiality, rather than 'high' as assumed in the base score section [65]. Following some experimentation with the CVSS starting values for the 2017-143 vulnerability, the key modifier was found to be 'attack complexity'. As the WannaCry attack was network-based, automated and self-replicating, the attack complexity was changed from high to low, which resulted in a new base score of 9.4, so 'critical'.

In conclusion, the analysis undertaken above shows that Microsoft had not updated their CVSS entry for the MS 17-010 vulnerabilities in response to the WannaCry attack 12th May 2017, or the Eternal Blue exploit, released on 14th April 2017 [67]. Taken together, the apparent lack of updates by Microsoft to its NVD records, and the exceedingly low number of critical vulnerabilities it records in the NVD (only four in 2017 [76] versus the 236 it self-reported as critical [68]), make it clear that Microsoft's 2017 NVD entries, at a minimum, should be treated with extreme caution.

2.3.3 The WannaCry attack: the role of vulnerability 'stockpiling'

Just two days after the WannaCry attack struck the NHS, Microsoft's President [69] called into question the US government's policy of stockpiling vulnerabilities, highlighting that both the US Central Intelligence Agency and NSA had lost control of exploits resulting in "widespread damage". The NSA's UK equivalent, the government communications headquarters, or GCHQ, published its 'Equities Process', seeking to introduce a degree of transparency and oversight for decisions relating to whether vulnerabilities should be retained for use by the intelligence services or disclosed to the relevant vendor. Factors include the residual risk of not disclosing the vulnerability and also the risk of a retained vulnerability being 'discovered' and exploited by others [70].

2.4 THE NHS IN ENGLAND

The NHS is the publicly funded healthcare service for the UK and free at the point of use. The four countries that make up the UK each have devolved responsibility for the delivery of health services.

In England, the UK government, through the Department of Health and Social Care (DHSC), has responsibility for health spending as well as setting the outcomes expected. It had a budget of £126.9bn for the year April 2017 to March 2018 [71, p. 2]. In March 2017, the total staff headcount for the NHS in England was 1,187,125 [72].

Figure 3 NHS England structure [71, pp. 2–3], [73]

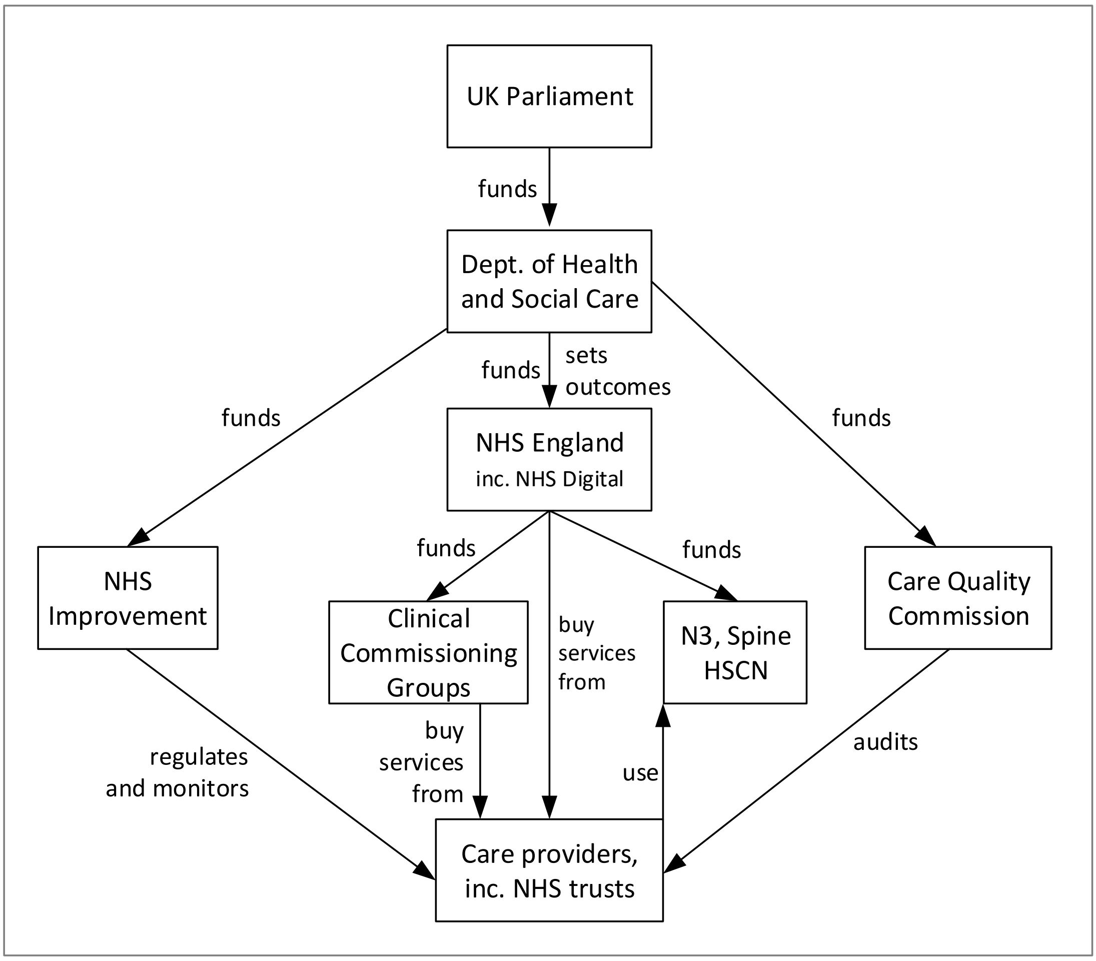


Figure 3 provides a simplified view of the NHS structure in England, as well as the funding flows. NHS trusts, such as the 153 hospitals trusts [4], are not directly funded by the DHSC; instead, they receive funding from NHS England, either directly, or via clinical commissioning groups. Trusts are regulated and monitored by NHS improvement. Auditing is the responsibility of the Care Quality Commission [73]. NHS Digital manages national health systems such as the ‘Spine’, which is a national patient database and the N3 and Health and Social Care Network (HSCN) data networks [5].

2.5 ENGLISH LOCAL GOVERNMENT

The 343 Local Authorities (LAs) in England had a combined budget of £117.8bn in the year 2017/18 [3]. LAs are funded by the Ministry of Housing, Communities and Local Government and through local taxation [3]. In December 2018, all the LAs in England employed a total of 1,570,600 staff [3]. Figure 4 shows the funding flows for LAs and the relationship with both the N3/HSCN networks and the public sector network (PSN).

Figure 4 English LA funding and relationships [3], [71, p. 3], [74]

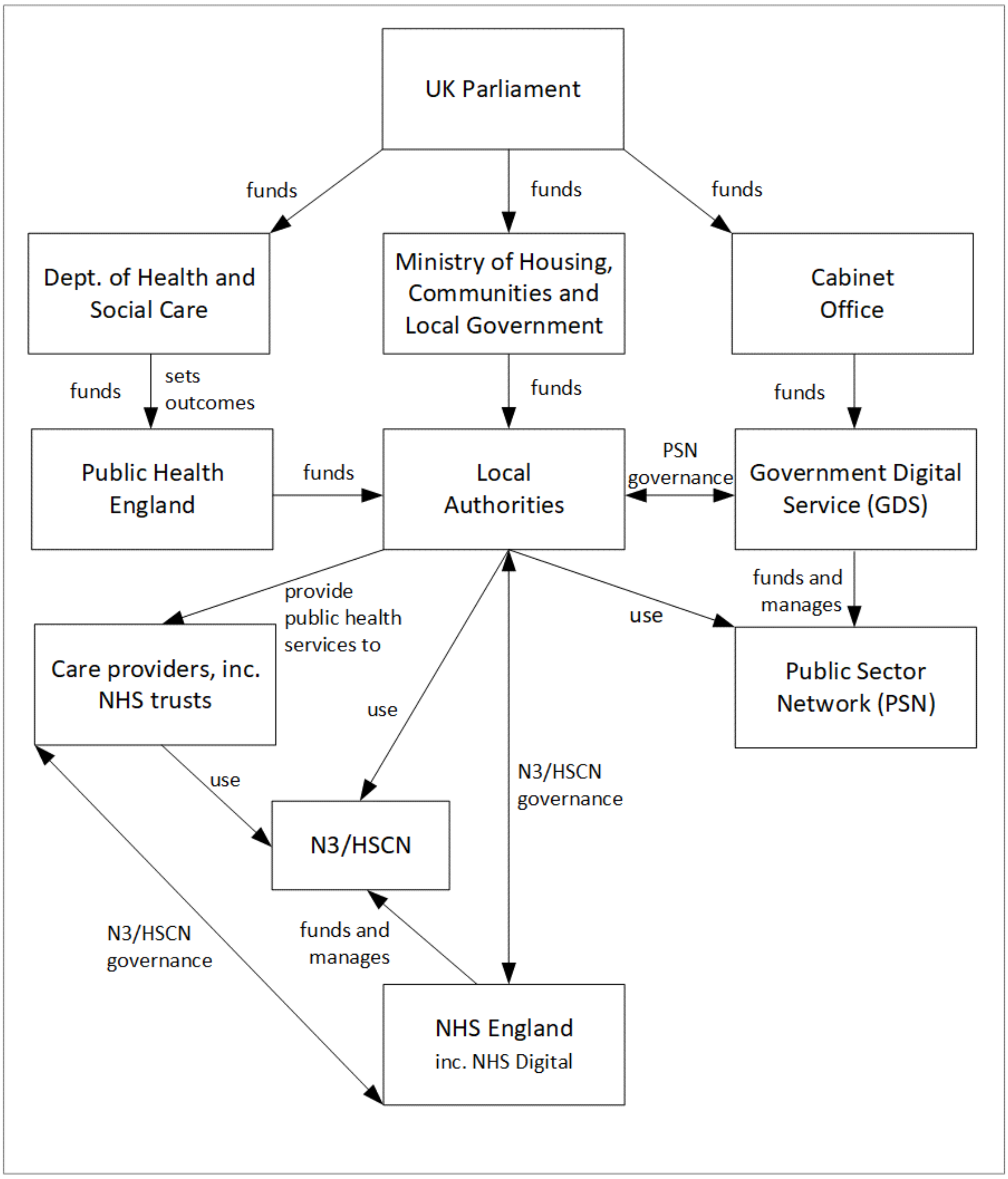

UK Parliament
funds
funds
funds
Dept. of Health and Social Care
Ministry of Housing, Communities and Local Government
Cabinet Office
funds
sets outcomes
funds
funds
Public Health England
funds
Local Authorities
PSN governance
Government Digital Service (GDS)
provide public health services to
funds and manages
use
Care providers, inc. NHS trusts
Public Sector Network (PSN)
use
use
N3/HSCN governance
N3/HSCN
N3/HSCN governance
funds and manages
NHS England inc. NHS Digital

Figure 4 also includes the NHS trusts' relationship with NHS Digital for the governance of N3 and HSCN.

2.6 NAO REPORT: "INVESTIGATION: WANNACRY CYBER-ATTACK AND THE NHS"

The NAO report [6] investigated the circumstances leading up to the WannaCry attack, its impact on NHS organisations and the probable causes. The report provides a comprehensive analysis of the organisations affected, including type, size and geography, and attempts to draw conclusions based on that data [6, pp. 16–19]. The report observed that affected organisations were running out-of-date or poorly patched versions of the Windows operating system, leaving the WannaCry code able to exploit a known software vulnerability. The difficulty of patching medical equipment is cited as the main reason for organisations not having up to date systems. The attack was not confined to internet connectivity, it “spread via the internet, including through the N3 network” [6, p. 11]. N3, or ‘New NHS Network’ is a private network currently in the process of being replaced by the new Health and Social Care Network (HSCN) [5]. The attack, therefore, had two potential points of ingress into NHS organisations. Unfortunately, how NHS organisations were infected is not explained in detail.

The report acknowledged that the intervention of an independent security researcher was instrumental in mitigating the attack through the activation of a ‘kill-switch’ on the evening of the 12th May 2017 [50], [6, p. 15]. The report also observes that organisations affected were likely to employ more staff than the NHS median, though could not establish what relevance this had [6, p. 19]. The NAO examined the guidance and oversight in place for NHS organisations before the attack and noted that “By 12 May, NHS Digital had inspected 88 out of 236 trusts and none had passed” [6, p. 19], and that “in general, trusts had not identified cyber-security as being a risk to patient outcomes” [6, p. 19]. Importantly, “NHS Digital cannot mandate a local body to take remedial action” [6, p. 6]. The report offers several ‘lessons learned’ including that effectively managed internet firewalls would have mitigated the attack, which implies that the attack was via a network boundary, though no data is offered to justify this claim.

The report also recommended that the NHS “ensure that organisations implement critical…alerts, including applying software patches and keeping anti-virus software up to date” [6, p. 25]. NHS Digital issues the alerts so can determine which patches it deems to be critical; however, the assessment of the vulnerability reporting process in section 2.3.2 demonstrated that care must be taken when relying on broad severity definitions such as ‘critical’ to inform a vulnerability management process. Any organisation relying on Microsoft’s 2017 ‘critical’ NVD entries, rather than its published vulnerability classifications would not have been protected from the WannaCry attack, assuming all other severities were ignored or deprioritised.

2.7 NHS REPORT: “LESSONS LEARNED REVIEW OF THE WANNACRY RANSOMWARE ATTACK”

The 1st February 2018 report from the NHS [2] acknowledges previous reports, although only the NAO report [6] is acknowledged explicitly [2, p. 7]. It claims that the attack did not specifically target the NHS and that “network firewalls facing the N3 network would have guarded organisations against infection” [2, p. 8]. The footnote in the NHS report refers to the NAO report, describing the attack as originating from both N3 and the internet [6, p. 11] but only recommends action concerning internet firewalls [6, p. 25]. This advice is somewhat too narrow, given that some NHS trusts were infected via their N3 connection. A better recommendation would have been that all organisational or security network boundaries that justify a firewall, e.g. N3, should be appropriately secured.

As part of its response to the attack, on 16th May 2017, NHS Digital issued an alert to its ‘CareCERT’ subscribers requesting that organisations apply the patches required to prevent WannaCry, as well as confirm that this activity had been carried out [6, p. 12]. A footnote also highlights that an alert was previously issued on 16th March 2017 when Microsoft first released the patches [59] and also on the 25th April 2017 following intelligence of a specific threat [6, p. 12].

The report has many recommendations. One of interest is that all NHS organisations have to comply with the Cyber Essentials Plus (CE+) certification by June 2021 [2, p. 23]. Cyber Essentials (CE) is a scheme sponsored by the UK government’s National Cyber Security Centre (NCSC) [75] that has two tiers. The first ‘basic’ level consists of a questionnaire that applicants complete and provide to an auditor for approval; the second ‘Plus’ certification, requires the basic CE certification and an on-site audit by an external auditor who tests the organisation’s security [76]. The use of an existing, external (though still government-backed) scheme is a sensible step as it both reduces the compliance load on the NHS and provides an independent assessment of each organisation’s security.

It is notable that the CE certification explicitly manages the risk of confusion between vendors and CVSS severities discussed in section 2.3.2 in two ways. First, patches are applicable where “the product vendor describes [the severity] as ‘critical’ or ‘high risk’”. Second, there are explicit instructions on CVSS metrics and their values that would constitute a ‘critical’ or ‘high risk’ vulnerability [77, Sec. Patch management]. The only weakness in the CE approach is that lack of direction for patches that are neither critical nor high risk, which is still likely to account for a considerable number of vulnerabilities.

A search of the CE web-based register for the word "trust" shows eleven NHS hospital trusts with CE and six with CE+ [78]. For the supply of IT services to General Practitioners (GPs) the report requires that suppliers are certified to ISO27001 [2, p. 24], a standard, it should be noted, that the NHS does not hold itself to.

2.8 UK PARLIAMENT REPORT: "CYBER-ATTACK ON THE NHS"

The Parliamentary Accounts Committee (PAC) issued a report on 28th March 2018 [43]. The report agreed with the recommendations in the previous NAO and NHS reports, though it takes a broader view in wanting their application across government, rather than just the NHS [43, p. 7]. The reports notes that the security audits undertaken by NHS Digital had increased to 200 trusts, up from the 88 in the NAO report [6, p. 6], with still no trust passing, though the CE+ standard used for the audit was described as a "high bar" [43, p. 10]. Information on the use of Windows XP was also provided; from 18% of systems in 2015, 4.7% in May 2017 and 1.8% when the PAC report was written. Windows XP was 'end-of-life', so no longer supported or patched, on 8th April 2014 [79], though the UK government did agree on an extended support agreement with Microsoft for a further year [80]. Windows XP was not receiving patches for almost three years at the time the PAC report was published, and NHS Digital only committed to "plan to remove or isolate unsupported software in the NHS – including Windows XP (by April 18)" [2, p. 17].

2.9 SUMMARY

Up until the WannaCry attack, malware had perhaps been treated as a 'fact of life' and not perceived as anything more than an occasional, low impact threat. There was no apparent 'ramping up' of the threat from ransomware before the 12th May 2017.

The three UK government reports, and the NAO report, in particular, provided insight into the likely causes of the WannaCry attack's success:

1. Failure to patch promptly [6, p. 25].
2. Failure to keep anti-virus software up to date [6, p. 25].

3. Failure to manage the risk from obsolete equipment that was ‘unpatchable’ [6, p. 16].
4. Weak firewall/boundary controls for the internet and N3 [6, p. 11].

While there is no evidence that the NHS was explicitly targeted, its size and complexity perhaps made it uniquely vulnerable. Though section 2.5 shows that LAs have a similar budget and collectively employ more staff than the NHS.

All NHS trusts in England were interconnected via N3, and it is possible that as a private network with outbound-only internet controls, some connected organisations placed too much trust in it. This, in turn, may have led to NHS trusts deploying network defences on their N3 boundary that were ‘softer’ than their internet boundary. Even the HSCN, which is replacing N3, offers no more security assurance than N3, though HSCN does improve security monitoring with both internal (Network Analytics Services, or NAS) and internet boundary (Advanced Network Monitoring, or ANM) security monitoring services in place [81]. If NAS and ANM had been present within N3, they might have provided NHS Digital with an ‘early warning’ of the WannaCry outbreak, as well as the forensic data to allow the source or ‘patient zero’ to be identified.

NHS Digital’s need to caveat their commitment to “remove or isolate unsupported software in the NHS – including Windows XP (by April 18)” with “plan to” [2, p. 17], despite retaining the option to ‘isolate’, perhaps indicates the scale of the issue NHS Digital was facing.

Chapter 3: Governance Analysis

3.1 APPROACH

This chapter first provides an overview of the ISO/IEC 27001:2013 Annex A controls, which are used within this project as the standard nomenclature for the WannaCry control failures, as well as for the analysis of the disparate, centrally mandated systems of governance in place for English NHS trusts and LAs. The applicability of the 'Cyber Essentials' scheme is also discussed.

3.2 ISO/IEC 27001:2013 ANNEX A CONTROLS

ISO/IEC 27001:2013 [7] (ISO 27001) is the international standard for information security management. A companion code of practice, ISO/IEC 27002:2013 [82] (ISO 27002) is also published and recommends security controls to support the requirements of ISO 27001. The ISO 27002 controls are summarised in ISO 27001 as 'Annex A', and it is this version of the controls used throughout this project. There are fourteen sets of controls numbered from 'A5' to 'A18', where the 'A' indicates Annex A. There are 114 controls within Annex A and organisations seeking certification to ISO 27001 must undertake a risk assessment and consider each of the controls.

There are areas of control overlap across Annex A, so the analysis within this chapter establishes 'primary' and 'secondary' controls, either in place, or judged to have failed. Strong primary and secondary controls imply a more comprehensive information governance system providing 'defence-in-depth', with weak or missing controls indicating the opposite. The Annex A control definitions are also used to map the root cause of the various breach data to a primary and, where necessary, secondary control failures.

Where necessary, the risk, or control, analysis undertaken by this project was simplified to include only the fourteen high-level control set definitions, rather than all 114 controls.

Table 3 summarises the fourteen Annex A control sets and their control coverage, in broad terms.

Table 3 ISO 27001 Annex A summary, from [7, pp. 10–22]

Annex A Reference	Summary of Control Set
A.5 Security Policy	Provides "management direction and support for information security."
A.6 Organisation of Information Security	"initiate and control the implementation and operation of information security" and "the security of teleworking and use of mobile devices".
A.7 Human Resource Security	Security of employees and contractors, prior, during and after employment.
A.8 Asset management	"identify organizational assets and define appropriate protection responsibilities."
A.9 Access control	"Business requirements of access control" and "prevent unauthorized access to systems and applications."
A.10 Cryptography	"To ensure proper and effective use of cryptography".
A.11 Physical and Environmental Security	"prevent unauthorized physical access, damage and interference to the organization's information".
A.12 Operations security	"Operational procedures and responsibilities" and "Technical vulnerability management".
A.13 Communications Security	"To ensure the protection of information in networks".
A.14 System Acquisition, Development and Maintenance	"Security requirements...an integral part of information systems across the entire lifecycle", "includes...services over public networks" and "security in development".
A.15 Supplier relationships	"To ensure protection of the organization's assets that are accessible by suppliers."
A.16 Information security incident management	"management of information security incidents, including communication on security events and weaknesses."
A.17 Information Security Aspect of Business Continuity Management	"security continuity shall be embedded in the organization's business continuity management systems.
A.18 Compliance	"Compliance with legal and contractual requirements" and "organizational policies and procedures".

3.3 CYBER ESSENTIALS

ISO 27001 Annex A has been chosen as the standard security control framework for governance analysis within this project, but it could be argued that the CE/CE+ scheme would be more suitable, given it is UK-centric, free to access and an emerging standard for compliance in the NHS [83]. However, a review of CE revealed limitations that made it less suitable for control analysis than ISO 27001 Annex A.

First, and most importantly, the scope of CE excludes non-electronic data, e.g. paper, cloud services and "bespoke and custom components of web applications" [77]. Some or all of which are likely to be present in large organisations, such as NHS trusts and LAs.

Second, CE is formed of mandatory control requirements and does not have the flexibility of risk management, e.g. mitigation or acceptance. It may, therefore, be less suitable for organisations that have mature information governance systems with risk management processes, such as those certified to ISO 27001. For example, CE states "Software must be…patched within 14 days of an update being released, where the patch fixes a vulnerability with a severity the product vendor describes as 'critical' or 'high risk'" [77]. While patching is the best mitigation for a software vulnerability, the 'must patch' approach of CE, rather than 'must patch or mitigate', excludes the opportunity to apply 'compensating controls', such as firewalls or intrusion prevention services, that may reduce the risk to a level that is tolerable to an organisation.

Finally, CE has no controls relating to obsolete or 'unpatchable' systems, and a failure to manage these was highlighted as a root cause within the NHS "lessons learned" [6, p. 18]. This is despite the NCSC, which manages the CE scheme, publishing guidance on managing the risks of using obsolete systems [84]. The reason for its exclusion is likely due to the NCSC's preference for the simplicity of control prescription within CE, rather than the relative complexity of control options, which its obsolete systems guidance provides.

3.4 WANNACRY: SECURITY CONTROL FAILURES

The UK government reports reviewed in the previous chapter highlighted the flaws in the NHS's information security management systems that allowed the WannaCry attack to succeed. For the purposes of this project all controls, and control failures, were standardised against the ISO 27001 standard, including Annex A. When analysing the WannaCry failures in the context of ISO 27001, the full 114 Annex A controls were considered, ensuring maximum control detail when reviewing the NHS and local government controls in later sections of this project. Information security governance may rely on multiple, overlapping controls, so the analysis also established ‘primary’ and ‘secondary’ controls. Accordingly, Table 4 was created to summarise the WannaCry root causes, with their respective ISO 27001 control ‘failures’. Defining primary and secondary control failures allows for more in-depth analysis of the governance systems in place over the later sections of this chapter.

Table 4 Project evaluation of WannaCry root causes using ISO 27001 [7]

WannaCry Attack: Root Causes	ISO27001 Primary	ISO27001 Secondary
Failure to patch promptly [6, p. 25]	A.12.6.1 "Management of technical vulnerabilities"	A.18.2 "Information Security Reviews"
Failure to keep anti-virus software up to date [6, p. 25]	A.12.2.1 "Controls against malware."	A.18.2 "Information Security Reviews"
Failure to manage the risk from obsolete equipment that was ‘unpatchable’ [6, p. 18]	Clause 6.1 "Actions to address risks and opportunities"	A.18.2 "Information Security Reviews"
Weak firewall/boundary controls for the internet and N3 [6, p. 11]	A.13.1 "Network Security Management"	A.14.1.2 "Securing application services on public networks"

The results of this analysis (Table 4) show that ISO 27001 Annex A had directly applicable controls for all but one root cause: the risk from obsolete systems. The general requirement to apply risk management (clause 6.1 of ISO 27001) was selected as the most suitable control. The emphasis on risk management within ISO 27001 is its main strength, as it allows any known threat to be risk managed. The frequency of 18.2 "Information Security Reviews” as a secondary control, which is within the A.18 compliance control set, underlines the importance placed on review and audit within ISO27001. Any failure of a primary control, such as A.12.2.1 "Controls against malware", should be detected through the review and audit controls required by A.18.

3.5 NHS ENGLAND SECURITY CONTROLS

The NAO report [6] highlighted that IT information governance within NHS trusts was the responsibility of the then Department of Health but the "…Department devolves responsibility for managing cyber-security to local organisations – NHS trusts, GPs, clinical commissioning groups and social care providers" [6, p. 21]. With the result that "NHS Digital cannot mandate a local body to take remedial action even if it has concerns about the vulnerability of that organisation" [6, p. 21].

3.5.1 The Information Governance Toolkit

The one point of control NHS England did have was as the gatekeeper to the national NHS network, N3. The information governance toolkit, or IGT, is the set of security controls that all N3 connecting organisations were required to complete and submit before joining the N3 service and then annually after that.

The toolkit consists of a baseline control set with applicability determined by the organisation applying. The application process is via a password-secured, online portal, though all the control tables are publicly available. This project reviewed the NHS Information Governance Toolkit literature available from 1st April 2014 to 1st April 2018 [85]. The IGT was replaced by the Data Security and Protection Toolkit (DSPT) from 1st April 2018 [86].

The IGT underwent revisions on a broadly annual basis throughout its life:

- Version 11 from 4th June 2013, 141 control requirements [87]
- Version 12 from 13th June 2014, 146 control requirements [88]
- Version 13 from 29th May 2015, 165 control requirements [89]
- Version 14 from 29th May 2016, 165 control requirements [90]
- Version 14.1 from 5th July 2017, 165 control requirements [91]

Version changes were well communicated, through news articles (cited above) that provided an overview of the changes as well as links to two further information sources. A 'release note' provided a summary of the changes made since that last version [92]. A 'control notice' detailed the changes between the previous and new IGT versions on a control-by-control basis [93], providing an excellent level of detail.

Regarding the number of controls within the IGT, the actual number of applicable controls varied according to the organisation. In version 14 (in force during the WannaCry attack) only 45 controls applied to an NHS 'acute' trust. LAs would be required to comply with only 28 controls. A review of the 45 trust controls showed 17 to be data protection focused.

Version 14 controls for "Acute" were compared against the WannaCry control failures documented in Section 3.2. To allow an assessment of the depth of control coverage in place, primary and secondary controls were selected from the IGT. The results of that analysis are provided in Table 5.

Table 5 Project evaluation of WannaCry root causes and IGT v.14 [90]

WannaCry Root Causes	NHS IGT Control Primary	NHS IGT Control Secondary
Failure to patch promptly [6, p. 25]	"14-323 All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures"	No suitable control
Failure to keep anti-virus software up to date [6, p. 25]	"14-311 Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code"	"14-323 All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures"
Failure to manage the risk from obsolete equipment that was 'unpatchable' [6, p. 18]	"14-301 A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and reviewed "	"14-307 An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy"
Weak firewall/boundary controls for the internet and N3 [6, p. 11]	"14-313 Policy and procedures are in place to ensure that Information Communication Technology (ICT) networks operate securely"	"14-323 All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures"

Table 5 shows that there was no explicit control requiring vulnerability management. A compensating, control was selected (14-323), though its reliance on ‘appropriate’ would have allowed organisations a degree of interpretation. This control could be considered a ‘catch-all’, given it was selected to mitigate three of the four root causes. The IGT control coverage in Table 5 is generally less precise than the ISO 27001 control equivalents in Table 4, so arguably provided less assurance that the root causes would be mitigated effectively.

3.5.2 Data Security and Protection Toolkit

The DSPT was effective from 1st April 2018 and published on a new, rebranded website. Like the IGT, the DSPT is portal-based and requires login authentication. Less data is publicly available compared to the IGT, however. For example, ‘version 1’ of the DSPT is not directly available. However, news items on ‘ISO27001 exemptions’, and a request for comments on version 2 of the DSPT and the release of the 2019/20 version (v1.9.6), are online and provided links to earlier versions of the DSPT [94], [95], [83]. The DSPT control structure is similar to the IGT, though the organisational applicability is much simpler, reducing the 15 defined organisation types within the IGT to just three, defined as ‘small’, ‘medium’, or ‘large’. An acute trust is ‘large’, and an LA is ‘small’. Unlike the IGT, all 116 controls, which are a combination of ‘assertations’ and evidential requirements, are applicable to an NHS trust. An IT health check (ITHC), which includes both an internal and external vulnerability assessment of connecting organisations, was also introduced within the DSPT.

Section 2.8 of this project highlighted the programme of testing within the NHS against Cyber Essentials Plus (CE+). The 2019/20 version of the DSPT, released on the 21st June 2019 incorporates CE+ controls, ahead of the CE+ becoming mandatory for all NHS trusts by “March 2021” [83].

The DSPT controls were analysed for applicability against the WannaCry root causes and the most suitable were selected as primary and secondary controls, to provide an indication of the depth of control coverage available. The assertions within the DSPT were used for primary controls; its extensive series of evidential requirements provided secondary controls. The results are provided in Table 6.

Table 6 Project evaluation of WannaCry root causes and DSPT v1.9.6 [83]

WannaCry Root Causes	DSPT Primary Control	DSPT Secondary Control
Failure to patch promptly [6, p. 25]	"Supported systems are kept up-to-date with the latest security patches."	"What is your approach to ensuring patches for critical or high-risk vulnerabilities are applied within 14 days of release?"
Failure to keep anti-virus software up to date [6, p. 25]	"All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway".	"Number of alerts recorded by the AV tool in the last three months."
Failure to manage the risk from obsolete equipment that was 'unpatchable' [6, p. 18]	"List of unsupported software prioritised according to business risk, with remediation plan against each item. "	"All software and hardware has been surveyed to understand if it is supported and up to date."
Weak firewall/boundary controls for the internet and N3 [6, p. 11]	"The organisation is protected by a well-managed firewall."	"The annual IT penetration testing is scoped in negotiation between the SIRO, business and testing team including a vulnerability scan…"

Table 6 demonstrates the highly specific control coverage within the DSPT, across both primary and secondary control areas, even compared to ISO 27002. Overall, the WannaCry root causes are wholly mitigated in-depth, provided the DSPT is fully complied with.

3.6 ENGLISH LOCAL GOVERNMENT SECURITY CONTROLS

The LA equivalent of the NHS IGT is the public sector network (PSN) compliance standard; it is managed by the Government Digital Service, (GDS), which is part of the UK government's Cabinet Office [74]. Version 1.31 was reviewed. It was issued on 12th March 2015, with three minor amendments up to 7th April 2017 [96]. There was no historical record of versions before 12th March 2015, in marked contrast to the decade-plus of historical data available on the IGT website.

The main elements of the PSN standard are the code of connection, or ‘CoCo’ and an ITHC [97]. The CoCo is principally an exception-based process. Policy guidance is provided in the relevant technology areas, and any exceptions must be documented, along with any mitigations put in place. As a compliance approach, it is entirely different from the focus on prescriptive controls within the IGT/DSPT.

The overlap of the IGT and PSN controls is the subject of an IGT news article from 21st January 2016 that reduces the exemptions PSN certificate holders (so LAs) have against the IGT control set [98]. The “simplification” of the PSN resulted in NHS Digital accepting less assurance against the IGT, which was then at version 13. The NHS data is typically thorough, with ‘before’ and ‘after’ control mappings [99].

It is notable that the version of the PSN CoCo reviewed for this project dates from 7th April 2017: just over a month before the WannaCry attack. The PSN CoCo controls were analysed for applicability against the WannaCry root causes. Again, primary and secondary controls were selected to provide an indication of the depth of controls available. The results are provided in Table 7.

Table 7 Project evaluation of WannaCry control failures and PSN V1.31 [97]

WannaCry Root Causes	**PSN CoCo IA Condition**	**PSN CoCo Secondary Control**
Failure to patch promptly [6, p. 25]	1a “Vulnerability management (patch management)”	7 “You must implement regular IT Health Checks (ITHCs)”
Failure to keep anti-virus software up to date [6, p. 25]	3 “include services to identify malware at the gateway”	3 “implement an equivalent level of protection at the end point.”
Failure to manage the risk from obsolete equipment that was ‘unpatchable’ [6, p. 18]	Security Gaps “mitigating the associated risk with an alternate arrangement “	1a “alternative mitigating action, such as disabling or reducing access”
Weak firewall/boundary controls for the internet and N3 [6, p. 11]	3 “You will ensure that your network has appropriately configured boundary protection”	7 “You must implement regular IT Health Checks (ITHCs)”

Table 7 provides evidence of adequate control coverage. Although not to the level of detail found in the DSPT, the WannaCry root causes would be fully mitigated, providing the PSN CoCo is fully complied with.

3.7 SUMMARY

The centrally mandated guidance in force for NHS trusts (IGT version 14) and LAs (PSN CoCo v1.31) at the time of the WannaCry attack differs significantly. In contrast to the PSN CoCo, the IGT did not provide full, explicit control coverage for the WannaCry control failures. The PSN CoCo also required an ITHC.

The difference in governance philosophy between GDS (that manages PSN) and NHS Digital is stark. From the 12th March 2015, GDS turned away from the control-focused approach of previous PSN CoCo versions [100] by creating an exception-driven scheme that is far simpler than both the IGT and more recent DSPT. NHS Digital's January 2016 downgrade of the PSN assurance equivalence against the IGT controls provides evidence of its opinion of GDS' change in direction.

Unsurprisingly, the DSPT, launched by NHS Digital in April 2018, eleven months after the WannaCry attack, provides full control coverage against the WannaCry control failures. An ITHC requirement was also added. From March 2021, NHS trusts will have to achieve certification to CE+, which will provide ongoing, external assurance of their security posture, assuming it will cover their scope fully and any ongoing flexibility they may require in control selection.

Chapter 4: Data Discovery Methodology

4.1 APPROACH

Analysis of publically available information security breach data from April 2014 to December 2017 for NHS hospital trusts and LAs in England, classifying root causes with applicable ISO/IEC 27002:2013 controls.

1. A search of Information Commissioner's Office (ICO) data for relevant breaches.
2. Undertake a general Google search for security breach reports for the NHS, focusing on 'Acute Trusts'.
3. Undertake a general Google search for security breach reports for local government organisations.

4.2 INFORMATION COMMISSIONER'S OFFICE DATA

Methodology: Google searches were made using various keywords, including "ICO" and "Breach". Search results that originated from the ICO or UK government websites were prioritised for analysis.

Since the introduction of the European Union's (EU) General Data Protection Regulation (GDPR) [101] on 25th May 2018 (incorporated in the UK Data Protection Act 2018), any individual or organisation that controls or processes personal data is required by law to report a 'breach' [102]. The ICO defines a breach as "…a security incident that has affected the confidentiality, integrity or availability of personal data" [103].

What constitutes a reportable breach to the relevant supervisory authority (the ICO in the UK) is subjective but described in the GDPR as likely to, "…result in a risk to the rights and freedoms of natural persons" [101].

Before the 25th May 2018, however, only certain bodies were legally required to report breaches. The EU Privacy and Electronic Communications (EC Directive) Regulations 2003 (or 'PECR') was amended by the UK government in 2011 to require reporting of data breaches from 26th May 2011 [104]. PECR primarily applies to electronic marketing, telecommunications providers and internet service providers, while including rules on the use of web browser ‘cookies’ [105]. No NHS or local government entity would, therefore, have been legally required to report data protection breaches before 25th May 2018.

4.2.1 ICO complaint data

The ICO has published data sets [106] that combine data protection and freedom of information complaints. These only exist for the period April 2014 to June 2018 and provide useful insights into the type of complaint submitted, including the sector, such as health and local government, and how they reach the ICO. Based on the 2014/15 data set as the earliest available baseline, there were 16,372 data protection complaints, with 1,073, or 6.5% categorised as a “self-reported incident”. The ICO’s annual report for 2017/18 [107] shows that data protection complaints have risen to 21,019, with 3,311, or 15.8% now self-reported, though the vast majority of complaints during these periods were still the result of third-party reporting, or audits undertaken by the ICO. In summary, the April 2014 to June 2018 data set provides an authoritative resource, allowing an analysis of the volume and type of complaints made by, or regarding, NHS and LA organisations.

4.2.2 ICO enforcement data

Each complaint case has a variety of outcomes that can arise from an ICO investigation, including ‘enforcement action’, for which further data is provided by the ICO [108]. Compared to the complaint data sets, the ICO website is constrained to a ‘rolling’ two years’ worth of data, with 125 available, from 17th July 2017 to 19th July 2019 [108], so all ‘post-WannaCry’. Using the sector filtering tool available on the ICO website, there were seven “Health” cases and six “Local Government”. Five of the health-related cases were against individuals, compared to only one local government case. This data set was deemed too narrow to justify further analysis.

4.2.3 ICO civil monetary penalty data

The most serious action the ICO can take is the issue of a notice for a civil monetary penalty (CMP), and an ICO data set was obtained for this [145]. Before 25th May 2018, the maximum penalty was £500,000. After the 25th May 2018, when the Data Protection Act (DPA) 2018 (and the GDPR) became law, it rose to the higher figure of 4% of an organisation's group revenue for the previous financial year, or €20million.

The CMP data set contained 214 records, from 22nd November 2010 to 17th July 2019. There were penalties applicable to contraventions of the successive versions of either the DPA [146] or the Privacy and Electronic Communications Regulations Act, or 'PECR' [147], which place restrictions on the use of personal data for marketing. The benefit of the CMP data is that the ICO provides a detailed notice that includes the result of their investigation into the root cause or causes. While the enforcement data reviewed in the previous section was limited to around one year of data, the imposition of fines on public bodies is newsworthy, so sources outside of the ICO were searched for the missing case detail.

A Google search of several older cases led to a website called "breachwatch.com" [109] which provided online access to copies of the ICO penalty notices for cases up to March 2015. BBC News reports were also searched and provided a reliable source of any data required between March 2015 and July 2017.

4.2.4 ICO security incident trends

From July 2016, the ICO published quarterly dashboard reports for data security incident trends [110], [111] in various formats: interactive websites, PDF and spreadsheets. The end-of-year 'Q4' reports for 2016/17 [112] and 2017/18 [113] are published as 'dashboard' reports on 'infogram.com'; each contained an embedded link to a raw data set for the whole year, that is otherwise not visible on the ICO website. The latest available reports are from April 2018 to September 2018 (2018/19 Q1 and Q2) [110], [111]. Importantly, all these data sets are focused on the DPA 1998 'principle seven' control failures and so provide the detail missing from the complaint data sets.

4.3 ORGANISATIONAL BREACH REPORTING: NHS ENGLAND

Methodology: Google searches were made using various keywords, including "NHS" and "Breach".

4.3.1 Influence of the Caldicott reports

The NHS is the custodian of the nation's health care records. It therefore stores and processes what may be some citizens' most sensitive personal data. In 1997, a committee led by Dame Fiona Caldicott issued a report [114] that codified the NHS' data protection responsibilities into six principles including; the need for staff to justify the use of personal data and to only access personal data on a need to know basis.

One innovation introduced by the report was the requirement that NHS organisations have a named individual that has ownership for data protection – this role became known as a 'Caldicott Guardian'. The Caldicott report preceded the Data Protection Act 1998, which introduced eight data protection principles [115], such as requiring that data is only processed for limited purposes and is kept secure. The close alignment between the Caldicott and DPA1998 principles is unlikely to be accidental. DPA1998 was based on the EU's Data Protection Directive that came into force in 1995 [116], although as a directive EU member states were not required to implement it as law directly. This is in contrast to the GDPR that, as an EU Regulation, automatically became law in all member states on 25th May 2018 [101].

In 2012 Dame Caldicott was invited to create a follow-up report [117] that focused on the perceived risks and issues of information sharing within the NHS, a theme that led to a new, seventh Caldicott principle that encouraged data sharing [118]. The report also took stock of data protection more generally. Chapter 4 of the report deals with "Personal Data Breaches" and the first section "Evidence of continuing laxity" perhaps speaks for itself. Having examined breaches between June 2011 and June 2012, the report goes on to describe breach reporting discrepancies between NHS organisations and the ICO, highlighting "…a need for a new, consistent reporting channel to ensure that breaches of patients' confidentiality do not escape the attention of senior managers, ministers, and regulators of health and social care" [118, p. 11].

4.3.2 NHS England incident reporting

The Calidcott report's recommendation for consistent breach reporting was implemented by the NHS in April 2013. The NHS Information Governance Toolkit (IGT) [119] provided security guidance for NHS and third-party organisations, including for breach reporting, until April 2018. The NHS in England has had a central information technology body since 2005, with the launch of the 'Health and Social Care Information Centre' (HSCIC) [120]. In July 2016, the HSCIC rebranded to NHS Digital [121]. Its website publishes details of all information governance incidents from June 2013 until May 2018 [122]. The reports are quarterly and include an explicit statement on referral to the ICO. A document issued on 1st June 2013 formalised the breach reporting benchmark as "…sufficiently high profile cases or deemed a breach of the Data Protection Act or Common Law Duty of Confidentiality" [123].

It is a standard of reporting that remained in place in the last version (5.1) of the guidance document issued on 29th May 2015 [124] and has the benefit of meeting the requirements of DPA 2018 by default. The guidance forms part of the toolkit documentation set [125]. As stated above, the IGT was replaced from April 2018 by the new Data Security and Protection Toolkit (DSPT), which has its own website [86]. The site publishes all breaches reported from 24th May 2018 (the day before the GDPR became law) [126]–[128] however, the format of these reports has been reduced to a table of sub-organisations with very high-level incident definitions. The new format is a significant departure from the detail available in the previous report format, which ended on 22nd May 2018 [129]. One benefit of the new style is that ICO submission rates for incidents are shown. For the 2017/18 Q2 and Q3 reports, these state that all incidents (122 and 307 respectively) were also reported to ICO. The 2017/18 Q4 report shows that only 15 of the 269 total incidents were not reported to the ICO.

In summary, the NHS centralised security incident reporting, pre-GDPR, provides a rich data source for incidents. Unfortunately, it is cumbersome to analyse due to a reporting format that relies almost entirely on unstructured, written incident reports. However, the high rate of onward reporting to the ICO means that the ICO's detailed security incident data, available from April 2016 to September 2018 [82], provides an authoritative resource for health data for mapping against ISO27002:2013 controls.

4.4 ORGANISATIONAL BREACH REPORTING: LOCAL GOVERNMENT

Methodology: Google searches were made using various keywords, including "Local Government", "Local Authorities" and "Breach".

4.4.1 LA reporting requirements

LAs do not benefit from a central IT advisory service equivalent to NHS Digital. The PSN CoCo does cover breach reporting in the form of a limited incident response requirement (section 1e); "…incidents that impact on the PSN, you must report them to the PSN team and other entities (GovCertUK, for example) as required" [96].

Health (the remit of the NHS) and social care (led by LAs) are closely intertwined: in January 2018 the Department of Health rebranded as the Department of Health and Social Care, centralising policy for both areas [130]. LAs are connected to the NHS network via the legacy N3 network, or the new HSCN [5]. Compliance with the IGT or Data Security and Protection Toolkit is therefore required, including the reporting of breaches to comply with the NHS guidance [124].

Section 2.2.2 highlighted the breach data provided by the NHS [122]. There is a seemingly one-off report created by NHS Digital for the 2015/16 year (1st June 2015 to 31st May 2016) [131] that applies analysis to the data captured from the incident reports. The report describes 681 total reported incidents with 305 (45%) originating from 'Acute Trusts', which include hospital settings; LAs reported eight incidents (1.2%) [131, p. 7]. The report goes on to speculate on this apparent disparity; "We cannot distinguish between organisations having few breaches due to their business model (e.g. pharmacies have no reason to put data at risk) and those that under-report (FOI [freedom of information] requests from the privacy lobby indicate that Local Authorities have as many incidents as the NHS but do not report them via the Reporting Tool)" [131, p. 7]. The report effectively offers 'conscientiousness' as a possible reason for the single incident reported by pharmacies (which numbered 10,178 connected organisations at 9th April 2016) [132], but not for the eight incidents reported by LAs (122 connected in the same period) [133]. Instead, freedom of information to LAs are mentioned, but not explicitly referenced.

Private organisations, even those operating public sector services such as pharmacies [134], are not within the scope of the Freedom of Information Act (FOIA), although in May 2018 the Committee for Standards in Public Life issued a report [135] that included a recommendation [135, p. 10] that the UK government consult on extending the FOIA to providers of public services.

4.4.2 Big Brother Watch report

An internet search for FOI requests that may have prompted the statement on LAs under-reporting revealed an August 2015 report from the campaign group 'Big Brother Watch' titled "A Breach of Trust: How local authorities commit 4 data breaches every day"[136]. This 200-page report surveyed every local authority in the UK using Freedom of Information requests to ask for details of personal data breaches over three years: 1st April 2011 to 1st April 2014. A 98% response rate is claimed

[136, p. 197] and data is provided over 182 pages, with the report's pdf format making the data challenging to interrogate directly. The report's sub-title is drawn from the 4,236 total breaches [136, p. 4] provided by the responding LAs divided by the three years covered by the report. While the title suggests that the report focused on the number of breaches, this is at odds with the FOI questions used to gather the data:

1. "The number of council personnel that have been convicted for breaches of the Data Protection Act.
2. The number of council personnel that have had their employment terminated for breaches of the Data Protection Act.
3. The number of council personnel that have been disciplined internally but have not been prosecuted for breaches of the Data Protection Act.
4. The number of council personnel that have resigned during disciplinary procedures.
5. The number of instances where a breach has not led to any disciplinary action." [136, p. 198]

What is apparent from these questions is the relative weight given to the potential punishment of staff arising from security breaches. Questions 1 to 3 are broadly similar, and the extra effort required to respond to each puts the request at risk of being refused on the grounds of cost. The ICO permits organisations to refuse an FOI request if the cost to comply with it would likely exceed £600 [137]. A search for "cost" in the report shows that 24 LAs used cost as grounds to exempt them from responding to all or part of the FOI request. The report does offer sensible recommendations [136, p. 3], including the need for standardised breach reporting. Since the 25th May 2018, the GDPR partly met the report's call for stronger sanctions resulting from breaches through its introduction of more substantial maximum fines for organisations: up to €20 million or 4% of annual revenue [138], up from the maximum £500,000 fine in place when the report was published. However, these organisation-focused sanctions may not have satisfied the report's stated desire for the prosecution of individuals.

The report does imply a considerable range of reporting behaviour; ten LAs accounted for over a third of the 4,236 total, with 1511 between them [136, p. 6]. 167 LAs provided a 'zero return' to the FOI [136, p. 10] and it is, of course, possible that at least some of these LAs were simply not ‘looking’ for breaches, or perhaps not encouraging staff to report them during the three years covered. The report recommended that the ICO issue an assessment notice to cover LAs, to match those provided to bodies such as the NHS [139]. The assessment notice was a provision in the DPA1998 that gave ICO additional audit powers [140].

Returning to the claims of under-reporting by LAs in the NHS Digital report of 2015/16 [131, p. 7], a search of the Big Brother Watch report for the word “health” returns four breaches, all from English LAs, so applicable to NHS England’s reporting. The FOI request did not request dates for breaches, nor explicit details of the type of data impacted, e.g. health, so it cannot be deemed to capture breaches relevant to the NHS authoritatively.

As stated previously, the breach data published by NHS Digital starts from 1st June 2013 [122] so only overlaps the 1st April 2011 to 1st April 2014 scope of the Big Brother Watch report [136] for nine months. The three relevant quarterly NHS Digital reports [141]–[143] total 100 incidents, 4, 31 and 65 respectively; which is perhaps an expected ‘ramping up’ for what was the first three-quarters of a new national reporting system. LA incidents only appear in the last relevant report, for 1st January 2014 to 31st March 2014, from Bristol City Council [143, p. 10] and two from Plymouth City Council [143, pp. 19, 21]. Searching the Big Brother Watch report for these councils shows a breach reported by Bristol City Council [136, p. 64] that closely matches the details of the incident reported to the NHS, Plymouth City Council refused to respond to the report’s FOI request on the grounds of cost [136, p. 86].

In conclusion, it is not possible to explicitly evidence underreporting of health-related breaches within the report, due to the absence of dates that allow cross-referencing and lack of detail on the data affected by the breaches.

4.4.3 LA reporting obligations to the NHS

The broader point made by the NHS Digital report on the sheer volume of breaches reported by LAs not appearing in the NHS reports [131, p. 7] is justified if LAs were required to report all breaches to the NHS, regardless of the type of data impacted. The NHS reporting guidance in place during the period of the Big Brother Watch report was at version 1 [144] from 1st January 2010 and version 2 from 1st June 2013 [123]. Version 1 has no reference to LAs, version 2 does refer to the history of breaches in both the NHS and LAs and defines the document's scope: "Organisations processing health and adult social care personal data" [123, p. 6]. LAs would be included in this definition, though it also implies an important qualification as LAs are substantial data owners in their own right, given the range of citizen services they provide.

The process for breach severity is also health-centric, reducing breach severity if clinical data is not at risk [123, p. 17]. The implication is that LAs may not consider reporting all breaches, whether they impacted NHS-data or not. While this is a possible explanation for the three LA breaches reported 1st June 2013 to 31st March 2014, there were several further updates to the NHS reporting guidance up to the date of the 2015/16 report; version 3 on 1st June 2014 [145], version 4 on 7th November 2014 [146], version 5 on 17th February 2015 [147], and a minor release, version 5.1 on 29th May 2015 [124].

Version 3 introduced an explicit guidance statement for LAs: "As a point of clarification, for Local Authorities, a key consideration is where Health-related data has been compromised and/or Care services may be impacted. In this case, such incidents should be reported using the HSCIC IG [information governance] SIRI [serious incidents requiring investigation] processes described in this guide" [145, p. 7]. This statement underlines the scope as being health data, rather than all data within an LA's control.

Version 4 maintained the scope of the guidance as above, though there is an amendment to the severity calculation [146, p. 19]. Whereas prior versions reduced severity where clinical data was not at risk or impacted, the guidance changed the definition to any personal data as defined by DPA1998. The change would allow the reporting process to treat LA and health data equally, though only if the scope were similarly broadened to include all LA data, not just health data.

Version 5 introduced a significant change for LAs: "As a point of clarification, for Local Authorities whilst we would recommend that all IG and Cyber SIRI are reported through this tool, a key consideration is where Health-related data has been compromised and/or Care services may be impacted" [147]. While this statement brought non-health data into the scope of the reporting guidelines, the use of the word "recommend" does not force or require LAs to adopt the NHS process for breach reporting. By convention, 'recommend' equates to guidance, so is deemed optional;

whereas ‘must’ obligates action. Even ‘Shall’ is considered ambiguous [148] and is to be avoided when drafting formal policies.

In summary, LAs have never been obligated to report non-health data related breaches through the NHS reporting process. However, as the data on non-health related breaches in LAs is only available either from the result of FOI requests[136] or ICO published data[106], there is a relative lack of transparency, compared to the NHS.

4.5 SUMMARY

Based on the review within this chapter of the literature and data available, there are five authoritative sources of security breach or incident data available for analysis:

- ICO ‘complaint’ data from 1st April 2014 to 30th June 2018;
- ICO civil monetary penalities data 22nd November 2010 to 17th July 2019;
- ICO data security trend data from 1st April 2016 to 30th September 2018;
- NHS England breach data from 1st June 2013 to 24th May 2018;
- Big Brother Watch Report from 1st April 2011 to 1st April 2014.

Only the ICO data sets will be further analysed within the next chapter of this project, for the reasons given below.

The Big Brother Watch report is the most comprehensive source of LA data but will be excluded due to its age (1st April 2011 to 1st April 2014). The report data only overlaps the NHS breach data by a matter of nine months, which would lead to a comparison of a limited data set that is more than five-years-old.

The NHS England breach data was also detailed, but cumbersome to analyse, given both the format and lack of data summarisation (aside from the “Annual IG Incident Trends 2015-2016” report). Breach data also tended to be focused on the ‘how’ of the incident or breach, rather than the ‘why’, which would provide the basis of establishing the root cause. The high rate of onward reporting to the ICO provides confidence that the ICO’s detailed security incident data, available from April 2016 to September 2018, is an authoritative source of NHS breach data.

While authoritative, the ICO security incident data is indicative of its focus on data protection (as required by successive data protection acts) rather than overall information security. Accordingly, organisations are not required to report information security incidents that do not impact data relating to a natural person. Even when a natural person is impacted by a security breach, there must be a serious risk of harm to that person before the breach justifies reporting to the ICO. Examples of information security events and incidents that would not necessarily require reporting are:

- A denial-of-service attack;
- malware that affects devices or equipment that do not process personal data, such as building management systems and perhaps even medical devices such as syringe drivers.

The ICO's data protection focus is a limitation of the ICO security incident data, but it is the only authoritative source of data for both health and LAs over a concurrent period: April 2016 to September 2018. Also significant is its relevance to the timing of the WannaCry attack (12th to 15th May 2017), which occurred roughly halfway through the 30-month data set (13½ months of data precede the attack, 16½ months follow it). The longer-term CMP data set provides an opportunity to analyse the actual root cause or causes found by an ICO investigation, so will also be analysed.

Page Intentionally Left Blank

Chapter 5: Data Analysis

5.1 APPROACH

This chapter will draw on the data sources selected in 4.5. The data will be analysed and standardised where necessary so that individual breach records or cases can be mapped against the appropriate ISO27002:2013 control set.

5.2 ICO COMPLAINT DATA

The following data sets were downloaded from the "Complaints and Concerns" section of the ICO website [106].

1. "2014/15 Data set: data set-201415.csv".
2. "2015/16 Data set: 201516-data set-1.csv".

From April 2016 monthly, rather than annual, reports were available. 27 reports were downloaded for analysis.

3. "Proactive disclosure of complaints report(s)" – April 2016 to June 2018

All data was downloaded from the ICO website in the 'comma-separated values' (CSV) format. The monthly reports were imported into Microsoft Excel using the data import feature. This created an Excel worksheet for each monthly report. The import process also added the Excel filtering feature to every worksheet, which was removed as it prevents some bulk operations.

The data sets contained 14 fields until the report for May 2016/17 (the second monthly report) when fields for financial year and month were added. Two extra blanks columns were added to the pre-May 2016/17 data sets so that the column layout was identical for all data. This aided the aggregation and bulk manipulation of the data.

Rather than work with two annual and 27 monthly data sets, the month worksheets were manually consolidated into financial years, giving the following data sets:

- 2014/15 – 21,735 records
- 2015/16 - 22,835 records

- 2016/17 – 24,272 records
- 2017/18 – 28,805 records
- 2018/19 Q1 - 7,729 records

For ease of use, the data sets required distillation into records only applicable to "Local Government" and "Health", which were pre-existing 'sector' values in the data. The data set fields were analysed for relevance; the results are summarised in Table 8.

Table 8 Project analysis of ICO complaint reporting fields

ICO Field Name	ICO Purpose	Relevance	Data Type	Notes
Case Reference	ICO case tracking	Unique identifier	Numeric	
Case type	Legislation and reporting detail	Analysis	Text	
Legislation	Abbreviated reference to Legislation	Filtering	Text	
Created date	ICO case tracking	None	'Short' Date	
Finished date	ICO case tracking	Analysis	'Short' Date	
Financial year	Financial year April to March	Analysis	Text	Only from May 2016
Month finished	Month case closed	Analysis	Text	Only from May 2016
Sector	Which of 44 sectors complaint subject is within	Analysis	Text	
Nature (1)	Complaint cause - primary	Analysis	Text	
Nature (2)	Complaint cause - secondary	Analysis	Text	
EIR technical breach	Environmental Information Regulations 2004	None	Text	
Exception	Legal basis for non-compliance with EIR	None	Text	
FOI Technical breach	Freedom of Information Act 2000	None	Text	
Exemption	Legal basis for non-compliance with FOI	None	Text	
Outcome	Action taken by data controller	Filtering	Text	
Submitted about party	Subject of complaint	Analysis	Text	

The process for applying the Table 8 analysis was as follows:

1. Removal of fields (worksheet columns) identified in Table 8 as having no relevance, i.e. Created Date, EIR technical breach, Exception, FOI Technical breach, Exemption.
2. Use of the Excel filter and ‘Go To’ features to delete records (worksheet rows) that do not apply to data protection legislation. An inverted filter was first applied to the Legislation column (everything but “DP”). Deleting this data would also delete any intervening rows hidden by the filter. To only select the unwanted, filtered data: ‘Go To’ (F5 key), ‘Special’ and ‘Visible data only’. Only the filtered data is selected, allowing it to be safely deleted using the ‘delete row’ feature so preserving the required data.
3. Use of the Excel filter feature to delete records (worksheet rows) that do not apply to Health or Local Government. The process for step 2 was repeated within the “Sector” column of the data sets, where there are 44 values.

Table 9 Project summary of ICO data sets

Data set	Total Records	Health Records	Health %	LA Records	LA %
2014/15	21,735	2,107	10%	1,847	8%
2015/16	22,835	2,765	12%	1,735	8%
2016/17	24,272	2,720	11%	2,067	9%
2017/18	28,805	3,384	12%	2,282	8%
2018/19 Q1	7,729	759	10%	631	8%
Totals	**105,376**	**11,735**	**11%**	**8,562**	**8%**

The data in Table 9 demonstrate a degree of consistency of both overall reporting volumes and the proportion of complaints that relate to Health and LAs.

As the aim of the analysis was to examine security failures, further filtering was undertaken to reduce the data sets to complaints that were deemed caused by a policy or control failure. The relevant field in the complaint record is “Outcome”. The various outcomes for ICO investigations are focused on the data controller (DC) or an organisation (org) described in the ICO document “Data protection case outcomes” [149]. These can range from “No action for DC”, to “CMP [civil monetary penalty] final notice served” (the most serious) and were evaluated for outcomes that indicated a security control failure. The evaluation of the outcomes is summarised in Table 10.

Table 10 Project evaluation of ICO case outcome applicability

ICO Case Outcomes from [149]	Indicates Control Failure?
“Descriptions of outcomes DC outside the UK”	No
“Not DPA”	No
“Concern to be raised with DC”	No
“Response needed from DC”	Yes
“No action for DC”	No
“General advice given to DC/org”	Yes
“Compliance advice given to DC/org”	Yes
“DC action required”	Yes
“Improvement action plan agreed”	Yes
“Monitored: sufficient improvement”	Yes
“Undertaking served”	Yes
“Advisory visit recommended”	Yes
“Compliance audit recommended”	Yes
“Preliminary enforcement notice served”	Yes
“Enforcement notice served”	Yes
“CMP notice of intent served”	Yes
“CMP final notice served”	Yes
“Insufficient information provided”	No

Of the five outcomes in Table 10 judged not to be indicative of a security failure, only “Concern to be raised with DC” appears to suggest a failure that may be relevant to this project. However, the outcome definition within the ICO guidance document [149] states “Used when a customer has raised a concern with us and we believe they should first have raised it with the data controller.” Hence the “Concern to be raised…” outcome describes a direction to the complainant, rather than to the ICO itself.

Table 10 was used to filter the data sets further, leaving only the complaints that are likely to have been caused by a security control failure.

A series of Excel ‘pivot tables’ were used to aggregate the primary “nature (1)” and the secondary “nature (2)” occurrences for each year, for both health and local government. Table 11 provides a list of the unique natures identified across the data sets, which have each been assessed for applicability from the perspective of confidentiality (C), integrity (I) and availability (A), or CIA. This discounted natures that relate explicitly to data protection, such as “subject access” and “use of data”, which are not.

Table 11 Project evaluation of ICO complaint nature and CIA applicability

ICO case natures	Security Control Failure?
Disclosure of data	Yes (C)
Electronic Communications	Yes (C, I)
Excessive/Irrelevant data	No
Fair proc. info not provided	No
FOI	No
Inaccurate data	Yes (I)
Notification	No
Obtaining data	No
Overseas transfers	No
Retention of data	No
Right to prevent processing	No
Security	Yes (C, I, A)
Subject access	No
Unable to identify	No
Use of data	No
None	No

Only four natures in Table 11 were deemed information security related. The prevalence of numerous data protection natures (eleven in total) is due to the ICO's leading role in enforcing the UK data protection act. All the natures (except for "Unable to identify" and those that are null, so defined as 'none') can be closely aligned to the eight data protection principles within the DPA1998 [115] which are summarised below.

1. "Personal data shall be processed fairly and lawfully…"
2. "Personal data shall be obtained only for one or more specified and lawful purpose…"
3. "Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed."
4. "Personal data shall be accurate and, where necessary, kept up to date."
5. "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."
6. "Personal data shall be processed in accordance with the rights of data subjects under this Act."

7. “Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”
8. “Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.”

Only the seventh principle in DPA1998 (the legalisation that applies to the whole data set) relates explicitly to information security management, in its role as underpinning all the data protection systems within an organisation. The other seven are concerned with aspects of the data lifecycle: gathering, processing, retention, and destruction. The data set complaint summaries are provided across three tables in Appendix A (Table 13, Table 14 and Table 15).

The data protection related elements were removed from the Appendix A table data; allowing the whole complaint data set to be summarised in Table 12. The ‘N1’ and ‘N2’ column headings indicate the count of the primary (N1) and secondary (N2) ICO natures within each year.

Table 12 Project analysis of ICO complaints relating to security failures

ICO ‘nature’	2014/15		2015/16		2016/17		2017/18		2018/19 Q1	
categories	N1	N2	N1	N2	N1	N2	N1	N2	N1	N2
Health										
Disclosure of data	258	28	350	41	424	77	1044	161	235	31
Elec. Comms	0	0	1	2	0	0	1	0	0	0
Inaccurate data	29	14	38	25	63	39	238	74	51	23
Security	104	103	126	145	178	157	658	286	151	29
Total	**391**	**145**	**515**	**213**	**665**	**273**	**1941**	**521**	**437**	**83**
Local Government										
Disclosure of data	270	49	201	30	300	44	320	67	135	20
Elec. Comms	0	0	0	0	0	0	0	0	0	1
Inaccurate data	40	6	44	28	44	33	58	26	29	15
Security	66	66	52	85	66	81	92	75	32	32
Total	**376**	**121**	**297**	**143**	**410**	**158**	**470**	**168**	**196**	**68**
Grand Total	**767**	**266**	**812**	**356**	**1075**	**431**	**2411**	**689**	**633**	**151**

The remaining data in Table 12 highlights the data protection-centric approach taken by the ICO. While the various elements of the data protection act are well represented in Appendix A table, this is not the case for ‘information security’ more generally, with the vital data missing an indication of the root cause. The remaining definitions were too broad to enable any meaningful analysis

In conclusion, the ICO complaint data sets provided minimal value for the purposes of establishing trends in security control failures for either the health or local government sectors.

5.3 ICO CIVIL MONETARY PENALTY DATA

The civil monetary penalty (CMP) data set contained 214 records, from 22nd November 2010 to 17th July 2019 [108]. As the focus of this project is the state of NHS England information security management, compared to English local government, records that did not apply to these entities were removed as follows:

- health: one for NHS Wales, one for Northern Ireland and four for entities that were either the private sector or not defined as trusts;
- local government: three records were for NHS Scotland and one for NHS Wales.

This filtering left nine records for health, all dated before the WannaCry attack (12th May 2017) and 25 for local government, so 34 records in total.

Each case was analysed for the root cause or causes, and a judgement was made regarding the primary and secondary Annex A control set affected. The results are presented in Appendix B: NHS trusts (Table 16) and LAs (Table 17). The ICO unique reference has been retained instead of the organisation name to preserve page space. The original ICO nature text from the CMP data set has been retained [150]. The data source was added, and abbreviated, within Table 16 and Table 17 as follows: breachwatch.com (BW); bbc.co.uk (BBC); ico.org.uk (ICO). Table 16 and Table 17 data were used to generate charts that highlight the primary and secondary control frequency for health (Figure 5) and LAs (Figure 6).

Figure 5 Frequency of Annex A control sets in Table 16: ICO CMP NHS data

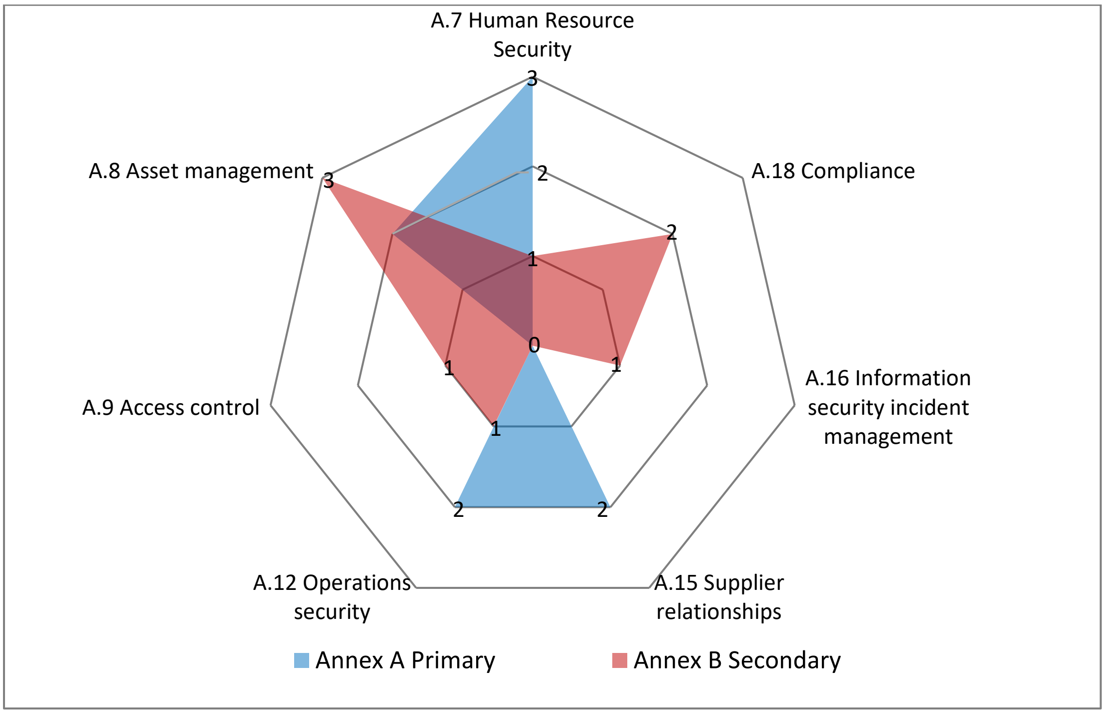
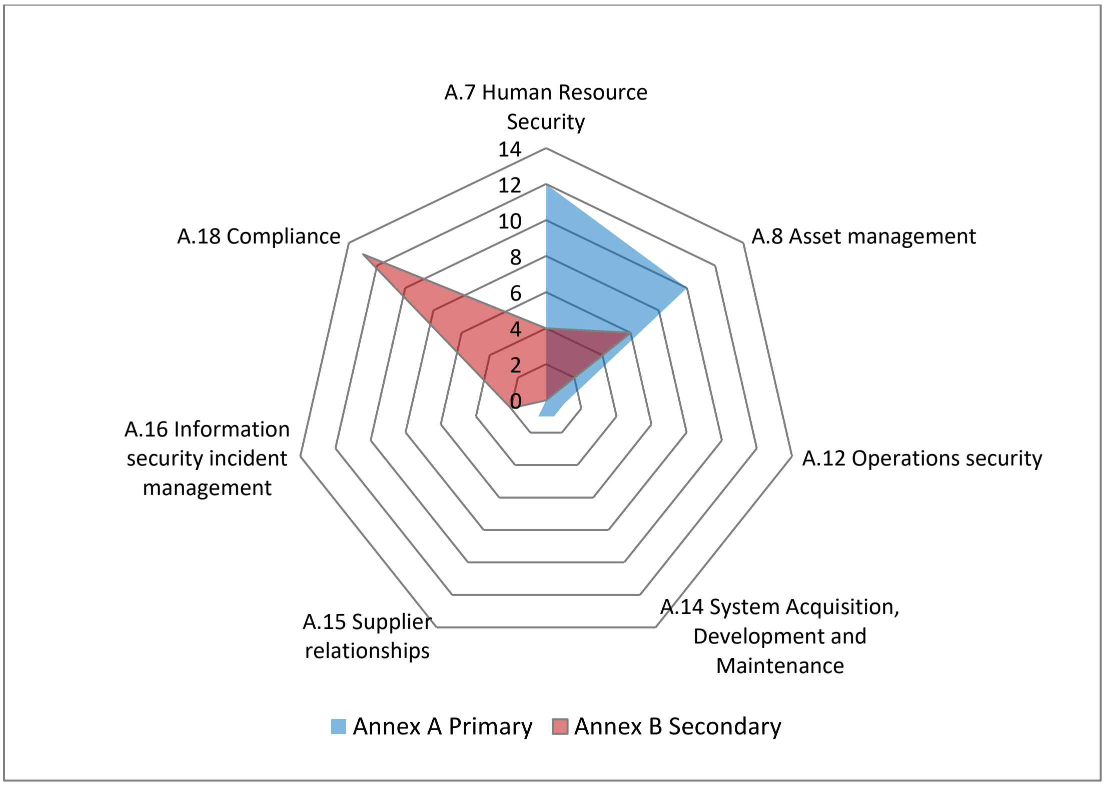


Figure 6 Frequency of Annex A control sets in Table 17: ICO CMP LA data



Observations from the analysis of the health (Table 16 and Figure 5) and LA (Table 17 and Figure 6) data:

1. Six out of seven control sets are the same in both sector data sets, so around half of the fourteen Annex A control sets. The types of cases that attract ICO fines may explain this similarity. The project author’s judgement and experience may have also influenced the application of the controls.
2. A.7 (human resource security) includes the training of staff (A.7.2.2), which is a recurring theme in the ICO reports.
3. A.8 (asset management) includes the requirement to classify (A.8.2.1), label (A.8.2.2) and control the handling of assets (A.8.2.3). Many of the breaches concerning the accidental release of information have their root cause in failure(s) to apply this group of controls.
4. A.18 (compliance) can be applied to every breach at some level, as it requires both internal compliance auditing of policies and procedures (A.18.2.2) and the technical review of systems against those policies and procedures (A.18.2.3). Where a primary control was failing, A.18 would also be a common secondary failure.

A key point from the 34 ICO cases analysed for health and local government is that all the fines levied were due to a contravention of the seventh data protection principle of DPA 1998 [115]: “Appropriate technical and organisational measures shall be taken…”. All are failures of information security management, so ultimately due to human factors: whether a single personal mistake, e.g. “ENF0441312, Personal data left on a train” [151], or systemic failures of design, operation and auditing of a service, e.g. “COM0602800, North London council fined after parking ticket system flaw leaves personal information at risk” [152].

The nine NHS trusts that received a CMP from the ICO were cross-referenced with the 32 trusts infected during the WannaCry attack [6, p. 30]. Only one, Blackpool Teaching Hospitals NHS Foundation Trust (COM573514 in Table 16), appeared in both. The underlying control failures that the author judges to have led to the CMP for that trust (A.8 asset management and A.9 Access control) do not appear in Table 4 Project evaluation of WannaCry root causes using ISO 27001 [7], which were failures of A.12 operations security, A.13 communications security and clause 6.1 risk management.

5.4 ICO SECURITY INCIDENT TRENDS APRIL 2016 TO SEPT. 2018

The lack of root cause detail within complaints investigated by the ICO has been dealt with, in part, by its publishing of on-line reports [110], [111] since July 2016 (2016/17 Q2). These reports have the express aim of educating organisations on security-related incidents. Raw data was available for April 2016 to Sept 2018 [110], [111], [112], [113].

The breach definitions within the data sets were found to be inconsistent across the 30 months of data, and even within the 2016/17 one-year data set [112]. Preparing the data for analysis revealed various issues that were also apparent within the 'complaint' data sets.

1. Consistent row naming but inconsistent data positions.
2. New or missing row names: five new definitions, including "Ransomware" were added in 2017/18.
3. Overly broad definitions, e.g. "Other principle 7 failure".

5.4.1 ICO security trend data from April 2016 to March 2018

The 2016/17 and 2017/18 data sets were sufficiently alike to allow the creation of Appendix C Table 18, which summarises them. The "N/A" entries in Table 18 show the "ICO incident/breach type" definitions introduced in the 2017/18 data set. The definition variations seen across the ICO data sets show the challenge of applying definitions reactively.

Table 18 data was used to generate charts that more clearly show the Annex A control set frequency failure for the NHS (Figure 7) and LAs (Figure 8).

Figure 7 ICO incident data NHS 2016/17 and 2017/18

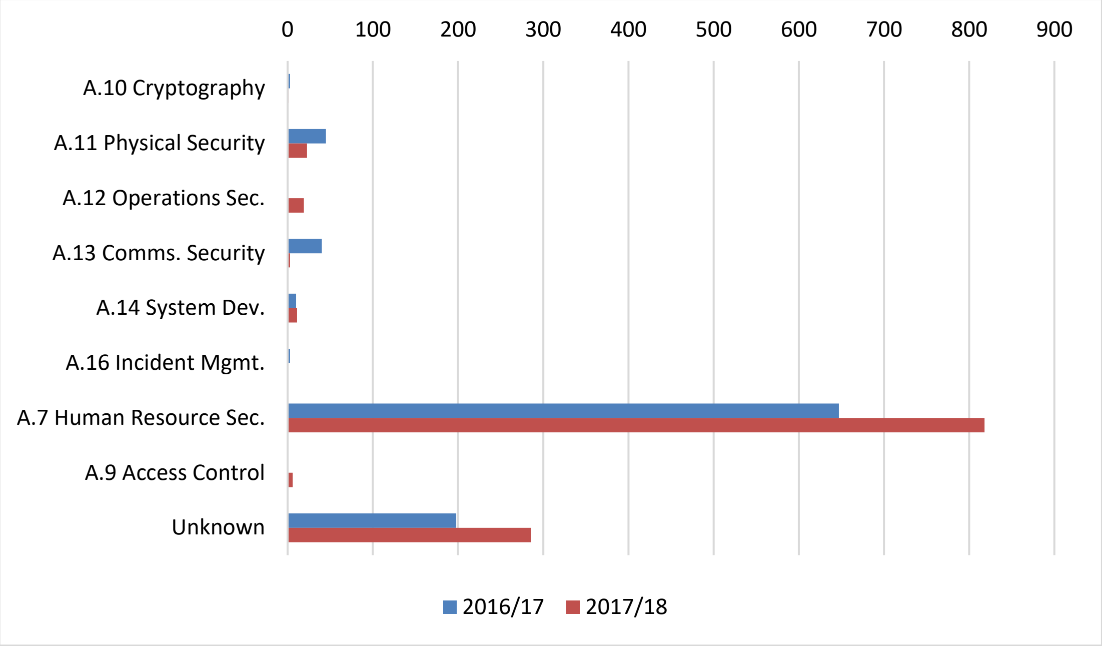
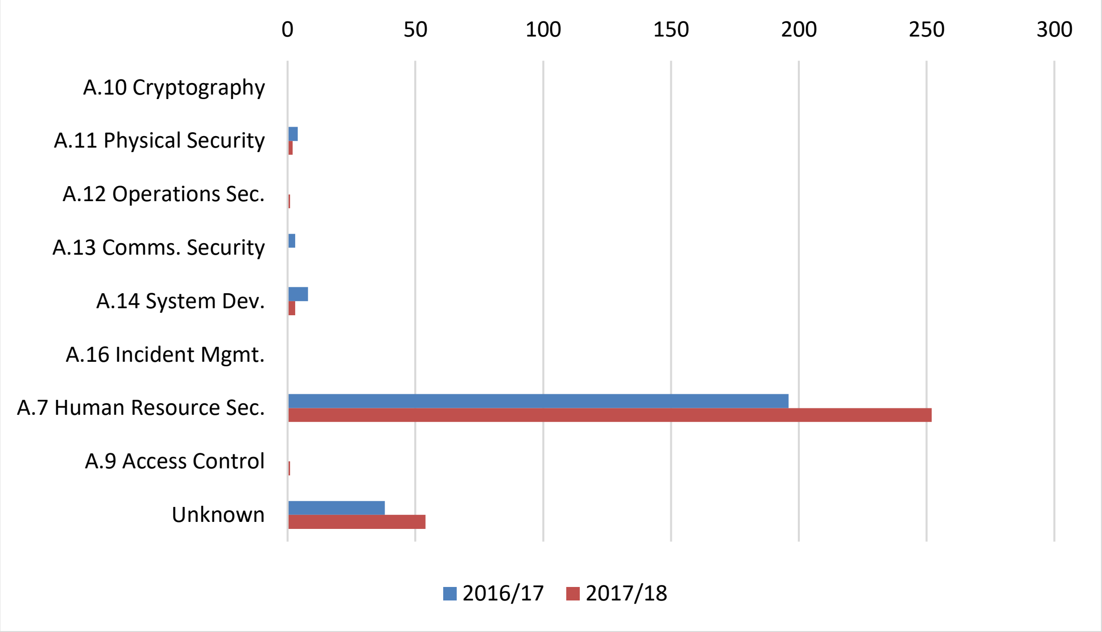


Figure 8 ICO security incident data for LAs 2016/17 and 2017/18



Observations from the analysis of Table 18 (all data), Figure 7 (NHS data) and Figure 8 (LA data):

4. There is no detail on the impacted organisations, so non-English entities cannot be excluded, which was possible for the complaint and CMP data sets.

5. The breach definitions only allow an Annex A control to be applied based on the primary control for the breach; however, the CMP analysis showed that the root cause could vary for the same headline breach type. For example, the primary control for “data left in insecure location” would be training staff to manage data safely (A.7 Human Resource Security); however, staff may have been trained, but still fail to follow the policy, which is a failure within A.18 compliance.
6. Unknown, which represents “Other principle 7 failure”, accounts for 23% of health and 16% of local government incidents.
7. The distribution of incident types is broadly similar for both health and local government.

5.4.2 ICO security trend data from April 2018 to September 2019

Unfortunately, the 2018/19 Q1 and Q2 data sets [110], [111] were a step backwards, from the perspective of recorded breach detail, as over 98% of both NHS and LA incident data were assigned a definition of either “Disclosure of Data” or “Security”. This data set was not analysed any further due to lack of meaningful detail.

5.5 SUMMARY

The ICO data sets suffer from a lack of standardisation, particularly regarding the root cause of incidents. Only the civil monetary penalty data set could be analysed authoritatively. Even then, most of the data were obtained from a third-party, ‘breachmaster.com’, which perhaps indicates the value the ICO places on its historical data. The use of broad definitions for breaches or complaints was a concern. “Other principle 7 failure” shows a failure of information governance and, surprisingly, the ICO does not judge the detail that lies behind almost a quarter of all health breaches between April 2016 and March 2018 valuable enough to share. More generally, the availability of only incident or breach descriptions in the ICO data sets, meant that the root cause data is only available in copies of ICO enforcement notices.

Despite the issues stated above, the data revealed broadly similar volumes year-on-year for NHS and LAs, with remarkably similar proportions and types of control failures.

Chapter 6: Conclusions

6.1 GOVERNANCE WEAKNESSES

It is telling that NHS Digital's post-WannaCry response was to turn to Cyber Essentials Plus (CE+), a generic information security certification available to any UK organisation, rather than directly audit organisations using its own, bespoke, IGT. CE+ includes the requirement for a third-party provided vulnerability assessment (ITHC) of both internal and external IT infrastructure. The ITHC not only sets CE+ apart from the basic CE certification but also the NHS IGT, which, like CE, is a scheme that lacks ongoing, external verification.

That no NHS trust could achieve CE+ certification during the period covered by the NHS and PAC reports suggests NHS Digital's information governance approach was not managing risk adequately, and furthermore, the trusts' impacted by the WannaCry had security weaknesses that the IGT failed to control. This may be due, in part, to the IGT's weak coverage of the control failures that contributed to the WannaCry attack (Table 5). NHS Digital's lack of authority over NHS trusts' information security management [6, p. 6] meant that it was not empowered to enforce compliance. The DSPT that launched in April 2018 hugely increased the controls applicable to an acute trust: from 45 in the IGT v14 (in force during the WannaCry attack) to 116 in DSPT 2019/20 v2. The new controls also include the requirement for a third-party provided ITHC, which adds the external verification missing from the IGT.

In contrast to the wholesale governance changes made by NHS Digital since the WannaCry attack, GDS made no changes to PSN CoCo used by LAs over the same period. It can be inferred that GDS judge the PSN scheme to be adequate in protecting against the risk of another attack like WannaCry. With the benefit of hindsight, NHS Digital's January 2016 decision to downgrade the assurance it believed the PSN CoCo provided compared to the IGT could be considered hubristic; particularly when every NHS trust failed to certify to CE+, a certification that, in terms of control coverage, has more in common with the PSN CoCo than the IGT.

However, given the structure of the NHS, trusts bear the ultimate responsibility for their information security, and it is the author's opinion that organisations with multi-million-pound budgets should not have to be told to patch software or manage the risk from obsolete systems.

The 22 recommendations within the NHS lessons learned report [2], which include the rollout of the DSPT, should significantly improve the security posture of NHS trusts, if implemented consistently. This project, therefore, offers no governance recommendations beyond those in the NHS report.

6.2 VULNERABILITY REPORTING

Section 2.3.2 in this project highlighted the disparity between the severities Microsoft applied to vulnerabilities within its security bulletins and those that resulted from its submission to the NVD. The WannaCry attack was perhaps the highest profile cyber-attack in 2017 and Microsoft did not update the relevant NVD entries to reflect the increase in risk that resulted from the public availability of the Eternal Blue exploit, or even the WannaCry attack itself. Using the CVSS scoring system, updating the relevant vulnerabilities records after either event would have resulted in their severity moving from high to critical severity. While only Microsoft vulnerability data for 2017 was analysed by this project, caution is advised for all NVD entries. More generally, the use of vague severity descriptors such as 'critical' should be avoided. The CE certification's specification of both vendor severity levels and CVSS metric values [77, Sec. Patch management] is an example of good practice in this area.

6.3 SECURITY DATA REPORTING

The analysis of the various data sets in Chapter 5 indicated a similar pattern in the historical security control failures for both the NHS and LA's, and none aligned to the explicit control failures that enabled the WannaCry attack to succeed. There was, therefore, no trend in the historical data indicating that the NHS was particularly at risk from malware, though the variable quality of much of the data means that this conclusion is far from authoritative.

There is no benchmark for how breaches and complaints are reported beyond each organisation's methodology. While the NHS and ICO were the sources of multi-year data, the style of reporting was found to be specific to each organisation. The data analysed in this project indicated only partial attempts by the NHS and ICO to normalise reported data so that long term trends could be more easily identified. The NHS published detailed breach data until May 2018, which required organisations to provide the ‘who, what, where and when’ of an incident, but not the ‘why’, which would obviously speak to the root cause. No LA breach data was found outside of either, the “Big Brother Watch” report [136], which was obtained through FOI requests, or the ICO.

The ICO, in particular, was the source of high-volume data sets that provided detailed organisational data, but with weak incident data (section 5.2), or aggregated sector data with higher levels of incident detail (section 5.4). Only the relatively small ICO civil monetary penalty (CMP) data set of 34 cases provided the detail necessary for a determination of the root cause of control failures (section 5.3)

It is the author’s opinion that the difficulties encountered in analysing the data and the fact that all 34 CMP cases were security management failures [115], make a strong case for the ICO, or ideally the entire UK government, adopting a standard security control framework for the definition of security incident root causation.

6.4 LIMITATIONS

Most of the data sets analysed did not contain the detail necessary to determine the root cause of each breach or incident.

6.5 RECOMMENDATIONS

Based on the limitations found within this project, the author recommends the following actions.

1. The UK government specifies a standard for breach reporting that includes the requirement to explicitly state the root cause against one or more standard control sets, such as ISO/IEC27001:2013 Annex A, or Cyber Essentials.
2. The UK government aggregates and publishes its breach data in regular reports, e.g. annually, that show security control failures by the government sectors, such as central government, local government and health.
3. The UK government aggregates breach data provided to it by suppliers, that shows security control failures by supplier sector type.

4. All data is made available in a portable format, e.g. CSV, to allow more straightforward third-party analysis. The UK government has an existing scheme for making data publicly available [153].

Bibliography

[1] D. Lee, ‘Massive cyber-attack hits 99 countries’, 13-May-2017. [Online]. Available: https://www.bbc.com/news/technology-39901382. [Accessed: 20-Feb-2019].

[2] W. Smart and S. House, ‘Lessons learned review of the WannaCry Ransomware Cyber Attack’, NHS England.

[3] ‘Local Government Facts and Figures’, *LGIU: Local Government Information Unit*. [Online]. Available: https://www.lgiu.org.uk/local-government-facts-and-figures/. [Accessed: 20-Feb-2019].

[4] ‘NHS statistics, facts and figures - NHS Confederation’. [Online]. Available: https://www.nhsconfed.org/resources/key-statistics-on-the-nhs. [Accessed: 20-Feb-2019].

[5] ‘Health and Social Care Network (HSCN)’, *NHS Digital*. [Online]. Available: https://digital.nhs.uk/services/health-and-social-care-network. [Accessed: 17-Feb-2019].

[6] ‘Investigation: WannaCry cyber attack and the NHS - National Audit Office (NAO) Report’, *National Audit Office*. [Online]. Available: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/. [Accessed: 20-Feb-2019].

[7] IST/33/1, *BS EN ISO/IEC 27001:2017 - Information technology. Security techniques. Information security management systems. Requirements*. 2013.

[8] ‘WannaCry a signal moment, says NCA’, *ComputerWeekly.com*. [Online]. Available: https://www.computerweekly.com/news/450421936/WannaCry-a-signal-moment-says-NCA. [Accessed: 03-Aug-2019].

[9] M. Innes, ‘Signal crimes and signal disorders: notes on deviance as communicative action1’, *Br. J. Sociol.*, vol. 55, no. 3, pp. 335–355, Sep. 2004.

[10] ‘Ransomware’, *Wikipedia*, 02-Feb-2019. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Ransomware&oldid=881383378. [Accessed: 18-Feb-2019].

[11] ‘Google Trends’, *Google Trends*. [Online]. Available: https://trends.google.com/trends/explore?date=all&q=ransomware,Malware. [Accessed: 18-Feb-2019].

[12] ‘LibrarySearch @ Royal Holloway’. [Online]. Available: https://librarysearch.royalholloway.ac.uk/primo-explore/search?sortby=rank&vid=44ROY_VU2&lang=en_US. [Accessed: 20-Feb-2019].

[13] 'RHUL LibrarySearch string for section 2.3: Ransomware 218 results.' [Online]. Available: https://librarysearch.royalholloway.ac.uk/primo-explore/search?query=any,contains,ransomware,NOT&query=any,contains,WannaCry,AND&pfilter=dr_s,exact,00000101,AND&pfilter=dr_e,exact,20170511,AND&tab=tab1&search_scope=LSCOP_44ROY_ALL&sortby=rank&vid=44ROY_VU2&facet=tlevel,include,peer_reviewed&lang=en_US&mode=advanced&offset=0. [Accessed: 18-Feb-2019].

[14] 'RHUL LibrarySearch string for section 2.3: Ransomware 122 results.' [Online]. Available: https://librarysearch.royalholloway.ac.uk/primo-explore/search?lang=en_US&mfacet=tlevel,include,peer_reviewed,1&mfacet=topic,include,Computer%20Crimes,2&mfacet=topic,include,Computer%20Science,2&mfacet=topic,include,Computer%20Security,2&mfacet=topic,include,Computer%20Viruses,2&mfacet=topic,include,Cybercrime,2&mfacet=topic,include,Cybersecurity,2&mfacet=topic,include,Data%20Security,2&mfacet=topic,include,Internet%20Crime,2&mfacet=topic,include,Internet%20Security,2&mfacet=topic,include,Malware,2&mfacet=topic,include,Ransomware,2&mfacet=topic,include,Security,2&mfacet=topic,include,Security%20Management,2&mode=advanced&offset=0&pfilter=lang,exact,eng,AND&pfilter=dr_s,exact,00000101,AND&pfilter=dr_e,exact,20170511,AND&query=any,contains,ransomware,NOT&query=any,contains,WannaCry,AND&search_scope=LSCOP_44ROY_ARTICLES&sortby=rank&tab=articles&vid=44ROY_VU2. [Accessed: 18-Feb-2019].

[15] 'History of malicious programs'. [Online]. Available: https://encyclopedia.kaspersky.com/knowledge/history-of-malicious-programs/. [Accessed: 18-Feb-2019].

[16] 'Cyber crime: a review of the evidence', *GOV.UK*. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf. [Accessed: 19-Feb-2019].

[17] 'Virus Bulletin, January 1990', p. 20, 1990.

[18] A. Young and M. Yung, *Cryptovirology: Extortion-Based Security Threats and Countermeasures*. 1996.

[19] K. Martin, *Everyday Cryptography: Fundamental Principles and Applications*, 2nd ed. Oxford: Oxford University Press, 2017.

[20] Q. Chen and R. A. Bridges, 'Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware', *ArXiv170908753 Cs*, Sep. 2017.

[21] L. D. Paulson, 'IEEE News Briefs', *Computer*, vol. 38, no. 7, pp. 24–25, Jul. 2005.

[22] 'Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute', 31-Oct-2008. [Online]. Available: https://nakamotoinstitute.org/bitcoin/. [Accessed: 19-Feb-2019].

[23] K. Kirkpatrick, 'Financing the Dark Web', *Commun ACM*, vol. 60, no. 3, pp. 21–22, Feb. 2017.

[24] ‘How to use Bitcoin to add money to your Microsoft account’. [Online]. Available: https://support.microsoft.com/en-gb/help/13942/microsoft-account-how-to-use-bitcoin-to-add-money-to-your-account. [Accessed: 02-Jul-2019].

[25] L. Kelion, ‘Cryptolocker “infects 250,000 PCs”’, 24-Dec-2013. [Online]. Available: https://www.bbc.com/news/technology-25506020. [Accessed: 19-Feb-2019].

[26] K. Liao, Z. Zhao, A. Doupe, and G. Ahn, ‘Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin’, in *2016 APWG Symposium on Electronic Crime Research (eCrime)*, 2016, pp. 1–13.

[27] P. E. Chaudhry, ‘The looming shadow of illicit trade on the internet’, *Bus. Horiz.*, vol. 60, no. 1, pp. 77–89, Jan. 2017.

[28] ‘ESET releases new decryptor for TeslaCrypt ransomware’, *WeLiveSecurity*, 18-May-2016. [Online]. Available: https://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/. [Accessed: 19-Feb-2019].

[29] ‘TeslaCrypt: Following the Money Trail and Learning the Human Costs of Ransomware « TeslaCrypt: Following the Money Trail and Learning the Human Costs of Ransomware’, *FireEye*. [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/05/teslacrypt_followin.html. [Accessed: 19-Feb-2019].

[30] ‘ENISA Threat Landscape 2012 — ENISA’. [Online]. Available: https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape. [Accessed: 19-Feb-2019].

[31] ‘Phoenix: DGA-Based Botnet Tracking and Intelligence | SpringerLink’. [Online]. Available: https://link-springer-com.ezproxy01.rhul.ac.uk/chapter/10.1007%2F978-3-319-08509-8_11. [Accessed: 19-Feb-2019].

[32] ‘IBM Storwize USB Initialization Tool may contain malicious code - United States’, 26-Apr-2017. [Online]. Available: http://www.ibm.com/support. [Accessed: 18-Feb-2019].

[33] ‘IEEE News Briefs’, *Computer*, vol. 47, no. 12, pp. 16–20, Dec. 2014.

[34] ‘FBI Incidents of Ransomware on the Rise’, *Federal Bureau of Investigation*, 29-Apr-2016. [Online]. Available: https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise. [Accessed: 19-Feb-2019].

[35] P. Wenham, ‘Extra Care Needed’, *ITNOW*, vol. 58, no. 4, pp. 22–23, Dec. 2016.

[36] C. Simms, ‘A Matter of Survival’, *ITNOW*, vol. 58, no. 4, pp. 30–31, Dec. 2016.

[37] ‘KSN Report: PC ransomware in 2014-2016’. [Online]. Available: https://securelist.com/pc-ransomware-in-2014-2016/75145/. [Accessed: 18-Feb-2019].

[38] ‘KSN Report: Ransomware in 2016-2017 | Securelist’. [Online]. Available: https://securelist.com/ksn-report-ransomware-in-2016-2017/78824/. [Accessed: 18-Feb-2019].

[39] ‘KSN Report: Ransomware and malicious crypto miners in 2016-2018’. [Online]. Available: https://securelist.com/ransomware-and-malicious-crypto-miners-in-2016-2018/86238/. [Accessed: 18-Feb-2019].

[40] A. L. Young and M. Yung, ‘Cryptovirology: The Birth, Neglect, and Explosion of Ransomware’, *Commun ACM*, vol. 60, no. 7, pp. 24–26, Jun. 2017.

[41] A. L. Young and M. Yung, ‘On Ransomware and Envisioning the Enemy of Tomorrow’, *Computer*, vol. 50, no. 11, pp. 82–85, Nov. 2017.

[42] I. Yaqoob *et al.*, ‘The rise of ransomware and emerging security challenges in the Internet of Things’, *Comput. Netw.*, vol. 129, pp. 444–458, Dec. 2017.

[43] ‘Cyber-attack on the NHS inquiry’, *UK Parliament*. [Online]. Available: https://www.parliament.uk/business/committees/committees-a-z/commons-select/public-accounts-committee/inquiries/parliament-2017/nhs-cyber-attack-17-19/. [Accessed: 20-Feb-2019].

[44] ‘WannaCry RHUL LibrarySearch’. [Online]. Available: https://librarysearch.royalholloway.ac.uk/primo-explore/search?facet=tlevel,include,online_resources&facet=tlevel,include,peer_reviewed&lang=en_US&mfacet=topic,include,Security,1&mfacet=topic,include,Risk%20Management,1&mfacet=topic,include,Information%20Technology,1&mfacet=topic,include,Malware,1&mfacet=topic,include,Ransomware,1&mfacet=topic,include,Data%20Security,1&mfacet=topic,include,Cybersecurity,1&mfacet=topic,include,Cybercrime,1&mfacet=topic,include,Cyber%20Security,1&mfacet=topic,include,Computer%20Security,1&mfacet=topic,include,Computer%20Science,1&mfacet=topic,include,Computer%20Crimes,1&mfacet=topic,include,Bitcoin,1&offset=0&query=any,contains,wannacry%20AND%20cause&search_scope=LSCOP_44ROY_ARTICLES&sortby=rank&tab=articles&vid=44ROY_VU2. [Accessed: 20-Feb-2019].

[45] ‘More ransomware cases “likely on Monday”’, 14-May-2017. [Online]. Available: https://www.bbc.com/news/uk-39916778. [Accessed: 20-Feb-2019].

[46] N. Kshetri and J. Voas, ‘Do Crypto-Currencies Fuel Ransomware?’, *IT Prof.*, vol. 19, no. 5, pp. 11–15, 2017.

[47] ‘ETERNALBLUE: Windows SMBv1 Exploit (Patched)’, *SANS Internet Storm Center*. [Online]. Available: https://isc.sans.edu/forums/diary/22304/. [Accessed: 20-Feb-2019].

[48] ‘The WannaCry ransomware attack’, *Strateg. Comments*, vol. 23, no. 4, pp. vii–ix, Apr. 2017.

[49] S. Gibbs, ‘WannaCry: hackers withdraw £108,000 of bitcoin ransom’, *The Guardian*, 03-Aug-2017.

[50] ‘Finding the kill switch to stop the spread of ransomware - NCSC Site’. [Online]. Available: https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0. [Accessed: 20-Feb-2019].

[51] N. Scaife, P. Traynor, and K. Butler, ‘Making Sense of the Ransomware Mess (and Planning a Sensible Path Forward)’, *IEEE Potentials*, vol. 36, no. 6, pp. 28–31, Nov. 2017.

[52] ‘Free Ransomware Decryptors - Kaspersky Lab’. [Online]. Available: https://noransom.kaspersky.com/. [Accessed: 20-Feb-2019].

[53] A. Palisse, H. L. Bouder, J.-L. Lanet, C. L. Guernic, and A. Legay, ‘Ransomware and the Legacy Crypto API’, presented at the The 11th International Conference on Risks and Security of Internet and Systems - CRiSIS 2016, 2016, vol. 10158, pp. 11–28.

[54] M. Almgren, Ed., *Detection of intrusions and malware, and vulnerability assessment: 12th international conference, DIMVA 2015, Milan, Italy, July 9-10, 2015 ; proceedings*. Cham: Springer, 2015.

[55] ‘NVD - Information’. [Online]. Available: https://nvd.nist.gov/info. [Accessed: 20-Feb-2019].

[56] ‘NVD - Vulnerability Metrics’. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss. [Accessed: 20-Feb-2019].

[57] ‘Common Vulnerability Scoring System Version 3.0 Calculator’, *FIRST — Forum of Incident Response and Security Teams*. [Online]. Available: https://www.first.org/cvss/calculator/3.0. [Accessed: 20-Feb-2019].

[58] ‘CVSS v3.0 Specification Document’, *FIRST — Forum of Incident Response and Security Teams*. [Online]. Available: https://www.first.org/cvss/v3.0/specification-document. [Accessed: 19-Aug-2019].

[59] BetaFred, ‘Microsoft Security Bulletin MS17-010 - Critical’. [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010. [Accessed: 02-Feb-2019].

[60] ‘NVD - CVE-2017-0143’. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-0143. [Accessed: 20-Feb-2019].

[61] ‘NVD - CVE-2017-0144’. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-0144. [Accessed: 20-Feb-2019].

[62] ‘NVD - CVE-2017-0145’. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-0145. [Accessed: 20-Feb-2019].

[63] ‘NVD - CVE-2017-0146’. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-0146. [Accessed: 20-Feb-2019].

[64] ‘NVD - CVE-2017-0148’. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-0148. [Accessed: 20-Feb-2019].

[65] ‘NVD - modified CVSS v3 Calculator for 2017-143’. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2017-0143&vector=AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H. [Accessed: 20-Feb-2019].

[66] ‘NVD - 2017-143 with Temporal CVSS v3 Calculator’. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2017-0143&vector=AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H. [Accessed: 20-Feb-2019].

[67] ‘EternalBlue’, *Wikipedia*, 21-Feb-2019. [Online]. Available: https://en.wikipedia.org/w/index.php?title=EternalBlue&oldid=884336226. [Accessed: 21-Feb-2019].

[68] ‘2017 Microsoft Vulnerabilities Report | BeyondTrust’. [Online]. Available: https://www.beyondtrust.com/resources/whitepapers/2017-microsoft-vulnerabilities-report. [Accessed: 21-Feb-2019].

[69] ‘The need for urgent collective action to keep people safe online: Lessons from last week’s cyberattack’, *Microsoft on the Issues*, 14-May-2017. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/. [Accessed: 20-Feb-2019].

[70] ‘The Equities Process | GCHQ Site’. [Online]. Available: https://www.gchq.gov.uk/features/equities-process. [Accessed: 20-Feb-2019].

[71] ‘dhsc-annual-report-and-accounts-2018-to-2019.pdf’. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817370/dhsc-annual-report-and-accounts-2018-to-2019.pdf. [Accessed: 31-Jul-2019].

[72] ‘NHS Workforce Statistics - March 2017, Provisional statistics’, *NHS Digital*. [Online]. Available: https://digital.nhs.uk/data-and-information/publications/statistical/nhs-workforce-statistics/nhs-workforce-statistics-march-2017-provisional-statistics. [Accessed: 09-Aug-2019].

[73] ‘How is the NHS structured?’, *The King’s Fund*. [Online]. Available: https://www.kingsfund.org.uk/audio-video/how-new-nhs-structured. [Accessed: 18-Jun-2019].

[74] ‘Public Services Network (PSN)’, *GOV.UK*. [Online]. Available: https://www.gov.uk/government/groups/public-services-network. [Accessed: 21-Feb-2019].

[75] ‘Cyber Essentials’, *Cyber Essentials*, 26-Sep-2017. [Online]. Available: https://www.cyberessentials.ncsc.gov.uk/. [Accessed: 20-Feb-2019].

[76] ‘Certification’, *Cyber Essentials*, 27-Sep-2017. [Online]. Available: https://www.cyberessentials.ncsc.gov.uk/getting-certified/. [Accessed: 20-Feb-2019].

[77] ‘NCSC Cyber Essentials; Requirements for IT Infrastructure’, *Cyber Essentials*, 16-Oct-2017. [Online]. Available: https://www.cyberessentials.ncsc.gov.uk/about. [Accessed: 05-Aug-2019].

[78] ‘Cyber Essentials: Search for a certificate’, *Cyber Essentials*, 27-Sep-2017. [Online]. Available: https://www.cyberessentials.ncsc.gov.uk/cert-search/?query=trust&pageNum=1&pageSize=25. [Accessed: 20-Feb-2019].

[79] ‘Windows XP End of Support’. [Online]. Available: https://www.microsoft.com/en-gb/windowsforbusiness/end-of-xp-support. [Accessed: 20-Feb-2019].

[80] S. Gibbs, ‘UK government PCs open to hackers as paid Windows XP support ends’, *The Guardian*, 26-May-2015.

[81] ‘HSCN: Improving cyber security’, *NHS Digital*. [Online]. Available: https://digital.nhs.uk/services/health-and-social-care-network/new-to-hscn/improving-cyber-security. [Accessed: 03-Aug-2019].

[82] IST/33/1, *BS EN ISO/IEC 27002:2017 - Information technology. Security techniques. Code of practice for information security controls*. 2013.

[83] ‘NHS Data Security and Protection Toolkit Standard for 2019-20 (updated 21 June 2019)’. [Online]. Available: https://www.dsptoolkit.nhs.uk/News/51. [Accessed: 04-Aug-2019].

[84] ‘Obsolete platforms security guidance - NCSC’. [Online]. Available: https://www.ncsc.gov.uk/guidance/obsolete-platforms-security-guidance. [Accessed: 04-Aug-2019].

[85] ‘Interoperability Toolkit’, *NHS Digital*. [Online]. Available: https://digital.nhs.uk/services/interoperability-toolkit. [Accessed: 03-Feb-2019].

[86] ‘Data Protection and Security Toolkit’. [Online]. Available: https://www.dsptoolkit.nhs.uk/. [Accessed: 16-Feb-2019].

[87] ‘NHS IGT V11 is Now Live (04/06/2013)’, 04-Jun-2013. [Online]. Available: https://www.igt.hscic.gov.uk/NewsArticle.aspx?tk=435155471644262&lnv=1&cb=d415b16d-80a7-47fe-808e-b30fbea30bc8&artid=106&web=yes. [Accessed: 21-Feb-2019].

[88] ‘NHS IGT V12 is Now Live (13/06/2014)’, 13-Jun-2014. [Online]. Available: https://www.igt.hscic.gov.uk/NewsArticle.aspx?tk=435155471644262&lnv=1&cb=3b7e712a-3d78-4062-8543-65a7d8f52d4e&artid=119&web=yes. [Accessed: 21-Feb-2019].

[89] ‘NHS IGT V13 is Now Live (29/05/2015)’, 29-May-2015. [Online]. Available: https://www.igt.hscic.gov.uk/NewsArticle.aspx?tk=435155471644262&lnv=1&cb=84a0ebab-5e31-4c84-866c-0377a3c404f9&artid=138&web=yes. [Accessed: 21-Feb-2019].

[90] ‘NHS IGT V14 is Now Live (29/05/2016)’, 29-May-2016. [Online]. Available: https://www.igt.hscic.gov.uk/NewsArticle.aspx?tk=435155812233747&lnv=1&cb=4def2507-fa5f-4ffe-9e2c-52199d5b481d&artid=156&web=yes. [Accessed: 21-Feb-2019].

[91] ‘NHS IGT v14.1 is Now Live (5/7/2017)’, 05-Jul-2017. [Online]. Available: https://www.igt.hscic.gov.uk/NewsArticle.aspx?tk=435155471644262&cb=af2ebcd4-3fcc-4765-a263-ae23ac4c4de5&artid=171&web=yes. [Accessed: 21-Feb-2019].

[92] ‘NHS IGT V14.1 Release Note’, 2017. [Online]. Available: https://www.igt.hscic.gov.uk/WhatsNewDocuments/IGTV14.1-ReleaseNote-July%202017.pdf. [Accessed: 21-Feb-2019].

[93] ‘IGT Control Notice v14 to 14,1 Mapping’. [Online]. Available: https://www.igt.hscic.gov.uk/WhatsNewDocuments/IGTV14%20to%20V14.1-ControlNotice-July%202017.xls.

[94] ‘NHS DSPT updated ISO 27001 exemptions (Updated 04 December 2018)’. [Online]. Available: https://www.dsptoolkit.nhs.uk/News/6. [Accessed: 21-Feb-2019].

[95] ‘NHS DSPT for 2019/20 (18 January 2019)’. [Online]. Available: https://www.dsptoolkit.nhs.uk/News/43. [Accessed: 21-Feb-2019].

[96] ‘PSN Code of Connection v1.31’, Apr-2017. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/607288/PSN_Code_of_Connection_v1.31.odt.

[97] ‘IT Health Check (ITHC): supporting guidance’, *GOV.UK*. [Online]. Available: https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance/it-health-check-ithc-supporting-guidance. [Accessed: 04-Aug-2019].

[98] ‘NHS PSN/IGT Equivalence’, 21-Jan-2016. [Online]. Available: https://www.igt.hscic.gov.uk/NewsArticle.aspx?tk=435155573782289&cb=1fd34285-3733-40ca-ab3b-9a39397d5a02&artid=153&web=yes. [Accessed: 21-Feb-2019].

[99] 'NHS PSN IGT Matching v14 matching detail-'. [Online]. Available: https://www.igt.hscic.gov.uk/Resources/PSN%20IGT%20Matching%20v14%20matching%20detail-e647bb5d9e3745739f1265507685afd2.pdf. [Accessed: 21-Feb-2019].

[100] 'GCSx CoCo example June 2009'. [Online]. Available: https://www.whatdotheyknow.com/request/45259/response/114145/attach/5/Section%20D%20Q5%20Spreadsheet.pdf. [Accessed: 05-Aug-2019].

[101] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, vol. 119. 2016.

[102] 'Report a breach', 15-Feb-2019. [Online]. Available: https://ico.gov.uk/for-organisations/report-a-breach/. [Accessed: 16-Feb-2019].

[103] 'Personal data breaches', 29-Jan-2019. [Online]. Available: https://ico.gov.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/. [Accessed: 16-Feb-2019].

[104] 'The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011'. [Online]. Available: http://www.legislation.gov.uk/uksi/2011/1208/made. [Accessed: 16-Feb-2019].

[105] 'What are PECR?', 09-Jan-2019. [Online]. Available: https://icoumbraco.azurewebsites.net/for-organisations/guide-to-pecr/what-are-pecr/. [Accessed: 16-Feb-2019].

[106] 'ICO Complaints and concerns data sets', 05-Dec-2018. [Online]. Available: https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/. [Accessed: 16-Feb-2019].

[107] 'Annual reports', 06-Aug-2018. [Online]. Available: https://ico.gov.uk/about-the-ico/our-information/annual-reports/. [Accessed: 16-Feb-2019].

[108] 'Enforcement action', 10-Sep-2018. [Online]. Available: https://ico.org.uk/action-weve-taken/enforcement/. [Accessed: 26-Jul-2019].

[109] 'Breach Watch | Data breaches and regulatory activities'. [Online]. Available: http://breachwatch.com/. [Accessed: 01-Aug-2019].

[110] 'ICO Latest Data security incident trends', 14-May-2018. [Online]. Available: https://ico.org.uk/action-weve-taken/data-security-incident-trends/. [Accessed: 20-Aug-2018].

[111] 'ICO Data Security Trends: previous reports', 14-Nov-2018. [Online]. Available: https://ico.org.uk/action-weve-taken/data-security-incident-trends/previous-reports/. [Accessed: 21-Feb-2019].

[112] ‘ICO Data security incident trends Q4 2016/17 by Information Commissioner’s Office - Infogram’. [Online]. Available: https://infogram.com/data-security-incident-trends-q4-2016-1g4qpz70zglom1y. [Accessed: 21-Feb-2019].

[113] ‘ICO Q4 Data Security Incident Trends Q4 2017/18 by Information Commissioner’s Office - Infogram’. [Online]. Available: https://infogram.com/1pyype2mpgdmkps37rq0yl05v5cy000r517. [Accessed: 16-Feb-2019].

[114] ‘Caldicott Report’, Dec-1997. [Online]. Available: https://webarchive.nationalarchives.gov.uk/20130124064947/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf. [Accessed: 16-Feb-2019].

[115] E. Participation, ‘Data Protection Act 1998’. [Online]. Available: https://www.legislation.gov.uk/ukpga/1998/29/contents. [Accessed: 16-Feb-2019].

[116] ‘EUR-Lex - 31995L0046 - EN’, *Official Journal L 281 , 23/11/1995 P. 0031 - 0050;* [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046. [Accessed: 16-Feb-2019].

[117] ‘The Information Governance Review’. [Online]. Available: https://www.gov.uk/government/publications/the-information-governance-review.

[118] ‘Caldicott2 Principles’. [Online]. Available: https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx. [Accessed: 16-Feb-2019].

[119] ‘NHS IGT Home Page’. [Online]. Available: https://www.igt.hscic.gov.uk/Home.aspx?tk=435106741839119&cb=2441c3e4-55e7-46e8-af2a-a768a080e446&lnv=7&clnav=YES. [Accessed: 16-Feb-2019].

[120] ‘NHSU folds in arm’s length review’, *Digital Health,* 30-Nov-2004. [Online]. Available: https://www.digitalhealth.net/2004/11/nhsu-folds-in-arms-length-review/. [Accessed: 16-Feb-2019].

[121] ‘Our role and remit in the health service’, *NHS Digital*. [Online]. Available: https://digital.nhs.uk/about-nhs-digital/our-work/our-role-and-remit-in-the-health-service. [Accessed: 16-Feb-2019].

[122] ‘IG Publications’. [Online]. Available: https://www.igt.hscic.gov.uk/publications.aspx?tk=435107465761162&cb=52615f27-bbd6-4ba4-8f22-573e4f0ca233&lnv=14&clnav=YES. [Accessed: 16-Feb-2019].

[123] ‘NHS HSCIC Checklist Guidance for Reporting, Managing and Inv v2_0’. [Online]. Available: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20IG%20SIRI%20%20Checklist%20Guidance%20V2%200%201st%20June%202013.pdf. [Accessed: 21-Feb-2019].

[124] ‘NHS HSCIC SIRI Reporting and Checklist Guidance v5_1’. [Online]. Available: https://www.igt.hscic.gov.uk/resources/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf. [Accessed: 21-Feb-2019].

[125] ‘About the IG Toolkit’. [Online]. Available: https://www.igt.hscic.gov.uk/resources/About%20the%20IG%20Toolkit.pdf. [Accessed: 16-Feb-2019].

[126] ‘NHS DSPT Q2 2018 Incidents’. [Online]. Available: https://www.dsptoolkit.nhs.uk/News/Attachment/170. [Accessed: 18-Feb-2019].

[127] ‘NHS DSPT Q3 2018 Incidents’. [Online]. Available: https://www.dsptoolkit.nhs.uk/News/Attachment/168. [Accessed: 18-Feb-2019].

[128] ‘NHS DSPT Q4 2018 Incidents’. [Online]. Available: https://www.dsptoolkit.nhs.uk/News/Attachment/169. [Accessed: 18-Feb-2019].

[129] ‘NHS IGT Incidents Q2 Apr-May 2018’. [Online]. Available: https://www.igt.hscic.gov.uk/Publications/2018%20Q2%20Report%20of%20H&SC%20Closed%20Level%202%20IG%20Serious%20Incidents%20Apr%20to%20June%202018.pdf. [Accessed: 21-Feb-2019].

[130] S. Neville, ‘Jeremy Hunt’s beefed up social care role met with scepticism’, *Financial Times*, 09-Jan-2018. [Online]. Available: https://www.ft.com/content/fb350f6e-f53b-11e7-8715-e94187b3017e. [Accessed: 17-Feb-2019].

[131] J. Burleigh, ‘NHS IGT Annual Information Governance (IG) Incident Trends (2015-2016)’. [Online]. Available: https://www.igt.hscic.gov.uk/Publications/Annual%20IG%20Incident%20Trends%202015-2016%20-%20Final%20Report%2015-09-2016.pdf. [Accessed: 21-Feb-2019].

[132] ‘NHS ITG V13 Compliance Community Pharmcy Contractors’. [Online]. Available: https://www.igt.hscic.gov.uk/Publications/IGTV13_Report-CommunityPharm-DispAppContactors-09-04-2016-Published.xlsx. [Accessed: 21-Feb-2019].

[133] ‘NHS ITG V13 Compliant Local Authorities 9-4-16’. [Online]. Available: https://www.igt.hscic.gov.uk/Publications/IGTV13_Report-LocalAuthorities-09-04-2016-Published.xlsx. [Accessed: 21-Feb-2019].

[134] ‘ICO What is the Freedom of Information Act?’, 16-Jul-2018. [Online]. Available: https://icoumbraco.azurewebsites.net/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/. [Accessed: 18-Feb-2019].

[135] ‘The Continuing Importance of Ethical Standards for Public Service Providers’. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705884/20180510_PSP2_Final_PDF.pdf. [Accessed: 18-Feb-2019].

[136] ‘Big Brother Watch - A-Breach-of-Trust (PDF)’. [Online]. Available: https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/08/A-Breach-of-Trust.pdf. [Accessed: 16-Feb-2019].

[137] ‘When can we refuse a request for information?’, 25-Jan-2019. [Online]. Available: https://icoumbraco.azurewebsites.net/for-organisations/guide-to-freedom-of-information/refusing-a-request/. [Accessed: 17-Feb-2019].

[138] ‘ICO GDPR Overview’, 18-Jan-2019. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/. [Accessed: 17-Feb-2019].

[139] ‘Assessment Notices under the Data Protection Act 1998 - Extension of the Information Commissioner’s Powers - Ministry of Justice - Citizen Space’. [Online]. Available: https://consult.justice.gov.uk/digital-communications/ico-assessment-notices/. [Accessed: 17-Feb-2019].

[140] ‘MoJ Memo DATA PROTECTION (ASSESSMENT NOTICES) (DESIGNATION OF NATIONAL HEALTH SERVICE BODIES) ORDER 2014 2014 No. 3282’. [Online]. Available: http://www.legislation.gov.uk/uksi/2014/3282/pdfs/uksiem_20143282_en.pdf.

[141] ‘NHS IGT Incidents Q3 2013’. [Online]. Available: https://www.igt.hscic.gov.uk/Publications/2013-Q3_Report%20of%20H&SC%20Closed%20Level%202%20IG%20Serious%20Incidents_June%20to%20Sept.pdf. [Accessed: 21-Feb-2019].

[142] ‘NHS IGT Incident Q4 2013’. [Online]. Available: https://www.igt.hscic.gov.uk/Publications/2013-Q4_Report%20of%20HSC%20Closed%20Level%202%20IG%20Serious%20Incidents_Oct%20to%20Dec.pdf. [Accessed: 21-Feb-2019].

[143] ‘NHS IGT Incident Q1 2014’. [Online]. Available: https://www.igt.hscic.gov.uk/Publications/2014-Q1_Report%20of%20H&SC%20Closed%20Level%202%20IG%20Serious%20Incidents_Jan%20to%20March.docx. [Accessed: 21-Feb-2019].

[144] ‘DE Checklist v1’. [Online]. Available: https://www.igt.hscic.gov.uk/WhatsNewDocuments/IG%20SUI%20Checklist%20doc%20final%20(2).pdf.

[145] ‘HSCIC SIRI Reporting and Checklist Guidance v3’. [Online]. Available: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20%20IG%20SIRI%20Checklist%20Guidance_V3%200_Updated%20June%202014.pdf.

[146] ‘NHS HSCIC Checklist Guidance v4 0’. [Online]. Available: https://www.igt.hscic.gov.uk/resources/IGIncidentsChecklistGuidance.pdf. [Accessed: 21-Feb-2019].

[147] ‘NHS HSCIC Checklist Guidance v5_0’. [Online]. Available: https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf. [Accessed: 21-Feb-2019].

[148] H. Xanthaki, ‘Clarity, Precision, Unambiguity and the Legislative Sentence’, in *Drafting Legislation : Art and Technology of Rules for Regulation*, 1st ed., London: Hart Publishing, 2014, pp. 85–107.

[149] ‘ICO Data protection case outcomes’, 15-Jul-2019. [Online]. Available: https://ico.org.uk/media/about-the-ico/documents/1624914/dp-case-outcomes.pdf. [Accessed: 21-Feb-2019].

[150] ‘Action we’ve taken’, 19-Jul-2019. [Online]. Available: https://ico.org.uk/action-weve-taken/. [Accessed: 26-Jul-2019].

[151] BreachMaster, ‘London Borough of Lewisham | Breach Watch’. [Online]. Available: http://breachwatch.com/2013/01/01/london-borough-of-lewisham/. [Accessed: 01-Aug-2019].

[152] ‘London Borough of Islington’, 10-Sep-2018. [Online]. Available: https://ico.org.uk/action-weve-taken/enforcement/london-borough-of-islington/. [Accessed: 01-Aug-2019].

[153] ‘Find open data - data.gov.uk’. [Online]. Available: https://data.gov.uk/. [Accessed: 02-Aug-2019].

[154] BreachMaster, ‘Central London Community Healthcare NHS Trust | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/05/21/central-london-community-healthcare-nhs-trust/. [Accessed: 01-Aug-2019].

[155] BreachMaster, ‘Brighton and Sussex University Hospitals NHS Trust | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/06/01/brighton-and-sussex-university-hospitals-nhs-trust/. [Accessed: 01-Aug-2019].

[156] BreachMaster, ‘St George’s Healthcare NHS Trust | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/07/12/st-georges-healthcare-nhs-trust/. [Accessed: 01-Aug-2019].

[157] BreachMaster, ‘Torbay Care Trust | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/08/06/torbay-care-trust/. [Accessed: 01-Aug-2019].

[158] BreachMaster, ‘Stockport Primary Care Trust | Breach Watch’. [Online]. Available: http://breachwatch.com/2013/05/30/stockport-primary-care-trust/. [Accessed: 01-Aug-2019].

[159] BreachMaster, ‘North Staffordshire Combined Healthcare NHS Trust | Breach Watch’. [Online]. Available: http://breachwatch.com/2013/06/11/north-staffordshire-combined-healthcare-nhs-trust/. [Accessed: 01-Aug-2019].

[160] BreachMaster, ‘NHS Surrey | Breach Watch’. [Online]. Available: http://breachwatch.com/2013/06/18/nhs-surrey/. [Accessed: 01-Aug-2019].

[161] ‘Hospital trust fined for data breach’, *BBC News*, 04-May-2016. [Online]. Available: https://www.bbc.com/news/uk-england-lancashire-36203807. [Accessed: 01-Aug-2019].

[162] C. Foxx, ‘NHS trust fined over HIV patient leak’, *BBC News*, 09-May-2016. [Online]. Available: https://www.bbc.com/news/technology-36247186. [Accessed: 01-Aug-2019].

[163] BreachMaster, ‘Hertfordshire County Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2010/11/22/hertfordshire-county-council/. [Accessed: 01-Aug-2019].

[164] BreachMaster, ‘Ealing Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2011/02/08/ealing-council/. [Accessed: 01-Aug-2019].

[165] BreachMaster, ‘Hounslow Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2011/02/08/hounslow-council/. [Accessed: 01-Aug-2019].

[166] BreachMaster, ‘Surrey Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2011/06/09/surrey-council/. [Accessed: 01-Aug-2019].

[167] BreachMaster, ‘North Somerset Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2011/11/28/north-somerset-council/. [Accessed: 01-Aug-2019].

[168] BreachMaster, ‘Worcestershire County Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2011/11/28/worcestershire-county-council/. [Accessed: 01-Aug-2019].

[169] BreachMaster, ‘Croydon Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/02/13/croydon-council/. [Accessed: 01-Aug-2019].

[170] BreachMaster, ‘Norfolk Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/02/13/norfolk-council/. [Accessed: 01-Aug-2019].

[171] BreachMaster, ‘Cheshire East Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/02/15/cheshire-east-council/. [Accessed: 01-Aug-2019].

[172] BreachMaster, ‘London Borough of Barnet | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/05/15/london-borough-of-barnet-2/. [Accessed: 01-Aug-2019].

[173] BreachMaster, ‘Telford & Wrekin Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/06/06/telford-wrekin-council/. [Accessed: 01-Aug-2019].

[174] BreachMaster, ‘Stoke-on-Trent City Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/10/25/stoke-on-trent-city-council-2/. [Accessed: 01-Aug-2019].

[175] BreachMaster, ‘Leeds City Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2013/01/01/leeds-city-council/. [Accessed: 01-Aug-2019].

[176] BreachMaster, ‘Plymouth City Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2012/11/24/plymouth-city-council/. [Accessed: 01-Aug-2019].

[177] BreachMaster, ‘Devon County Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2013/01/01/devon-county-council/. [Accessed: 01-Aug-2019].

[178] BreachMaster, ‘Halton Borough Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2013/05/30/halton-borough-council/. [Accessed: 01-Aug-2019].

[179] BreachMaster, ‘Islington Borough Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2013/08/20/islington-borough-council/. [Accessed: 01-Aug-2019].

[180] BreachMaster, ‘North East Lincolnshire Council | Breach Watch’. [Online]. Available: http://breachwatch.com/2013/10/29/north-east-lincolnshire-council/. [Accessed: 01-Aug-2019].

[181] ‘Social care files left in sold building’, *BBC News*, 16-Aug-2016. [Online]. Available: https://www.bbc.com/news/uk-england-hampshire-37094976. [Accessed: 01-Aug-2019].

[182] ‘Council fined £150,000 for data breach’, *BBC News*, 31-May-2017. [Online]. Available: https://www.bbc.com/news/uk-england-essex-40110726. [Accessed: 01-Aug-2019].

[183] ‘Council fined £100k over mailbox hack’, *BBC News*, 12-Jun-2017. [Online]. Available: https://www.bbc.com/news/uk-england-gloucestershire-40247117. [Accessed: 01-Aug-2019].

[184] ‘Nottinghamshire County Council’, 10-Sep-2018. [Online]. Available: https://ico.org.uk/action-weve-taken/enforcement/nottinghamshire-county-council/. [Accessed: 01-Aug-2019].

[185] ‘The Royal Borough of Kensington and Chelsea’, 10-Sep-2018. [Online]. Available: https://ico.org.uk/action-weve-taken/enforcement/the-royal-borough-of-kensington-and-chelsea/. [Accessed: 01-Aug-2019].

Page Intentionally Left Blank

Appendices

Appendix A Project Analysis of ICO Complaint Data

Table 13 Project analysis of ICO complaint natures 2014/15 and 2015/16

	2014/15		2015/16	
Nature Definitions	**Nature (1)**	**Nature (2)**	**Nature (1)**	**Nature (2)**
Health				
Disclosure of data	258	28	350	41
Electronic Communications	0	0	1	2
Excessive/Irrelevant data	2	1	1	11
Fair proc. info not provided	12	1	12	1
FOI	0	0	0	0
Inaccurate data	29	14	38	25
Notification	1	1	4	2
Obtaining data	0	0	8	12
Overseas transfers	0	0	0	0
Retention of data	3	2	5	5
Right to prevent processing	4	1	49	2
Security	104	103	126	145
Subject access	436	27	603	276
Unable to identify	0	0	0	0
Use of data	4	4	16	11
None	149	820	14	694
Total	**1002**	**1002**	**1227**	**1227**
Local Government				
Disclosure of data	270	49	201	30
Electronic Communications	0	0	0	0
Excessive/Irrelevant data	5	5	2	2
Fair proc. info not provided	19	10	35	8
FOI	0	0	0	6
Inaccurate data	40	6	44	28
Notification	2	830	2	1
Obtaining data	2	3	5	7
Retention of data	2	4	3	5
Right to prevent processing	5	2	0	2
Security	66	66	52	85
Subject access	583	82	467	176
Unable to identify	0	0	0	0
Use of data	6	8	18	31
None	91	26	21	469
Total	**1091**	**1091**	**850**	**850**
Grand Total	**2093**	**2093**	**2077**	**2077**

Table 14 Project analysis of ICO complaint natures 2016/17 and 2017/18

	2016/17		2017/18	
	Nature (1)	**Nature (2)**	**Nature (1)**	**Nature (2)**
Health				
Disclosure of data	424	77	1044	161
Electronic Communications	0	0	1	0
Excessive/Irrelevant data	9	5	19	10
Fair processing info not provided	25	7	60	20
FOI	0	0	0	1
Inaccurate data	63	39	238	74
Notification	2	1	3	42
Obtaining data	7	15	22	27
Overseas transfers	0	0	3	0
Retention of data	3	11	29	15
Right to prevent processing	11	5	34	17
Security	178	157	658	286
Subject access	518	216	1199	178
Unable to identify	1	1	24	2
Use of data	10	14	50	25
None	5	708	0	2526
Total	**1256**	**1256**	**3384**	**3384**
Local Government				
Disclosure of data	300	44	320	67
Electronic Communications	0	0	0	0
Excessive/Irrelevant data	10	4	4	4
Fair processing info not provided	14	19	13	4
FOI	1	2	0	1
Inaccurate data	44	33	58	26
Notification	3	0	0	4
Obtaining data	9	18	11	23
Retention of data	5	8	6	8
Right to prevent processing	5	2	8	4
Security	66	81	92	75
Subject access	521	111	533	55
Unable to identify	0	0	5	0
Use of data	24	15	19	9
None	8	675	4	793
Total	**1010**	**1012**	**1073**	**1073**
Grand Total	**2266**	**2268**	**4457**	**4457**

Table 15 Project analysis of ICO complaint natures 2018/19 Q1

	2018/19 Q1	
	Nature (1)	**Nature (2)**
Health		
Disclosure of data	235	31
Electronic Communications	0	0
Excessive/Irrelevant data	1	1
Fair processing info not provided	7	5
FOI	0	0
Inaccurate data	51	23
Notification	0	29
Obtaining data	9	6
Overseas transfers	1	0
Retention of data	3	5
Right to prevent processing	11	2
Security	151	29
Subject access	266	22
Unable to identify	12	0
Use of data	12	4
None	0	602
Total	**759**	**759**
Local Government		
Disclosure of data	135	20
Electronic Communications	0	1
Excessive/Irrelevant data	7	2
Fair processing info not provided	7	3
FOI	0	0
Inaccurate data	29	15
Notification	0	3
Obtaining data	4	6
Retention of data	7	4
Right to prevent processing	6	1
Security	32	32
Subject access	225	5
Unable to identify	1	0
Use of data	13	5
None	0	369
Total	**466**	**466**
Grand Total	**1225**	**1225**

Appendix B Project Evaluation of ICO Civil Monetary Penalty Data

Table 16 Project evaluation of NHS Trust ICO CMP data using ISO 27001

ICO Ref	ICO Nature	Annex A Primary	Annex B Secondary	Source
ENF0406305	"Multiple faxes containing personal data sent to incorrect recipient".	A.7 Human Resource Security	A.8 Asset management	BW[154]
ENF0367593	"Insecure disposal of hard drives containing personal data".	A.15 Supplier relationships	A.18 Compliance	BW[155]
ENF0393565	"Personal data disclosed in error to incorrect recipient".	A.12 Operations security	A.7 Human Resource Security	BW[156]
ENF0414667	"Personal data published in error on Council's website".	A.12 Operations security	A.8 Asset management	BW[157]
ENF0425946	"Confidential waste bins and black plastic bags containing personal data discovered in decommissioned building".	A.8 Asset management	A.16 Information security incident management	BW[158]
ENF0417531	"Multiple faxes containing personal data sent to incorrect recipient".	A.7 Human Resource Security	A.12 Operations security	BW[159]
ENF0452677	"Insecure disposal of hard drives containing personal data".	A.15 Supplier relationships	A.18 Compliance	BW[160]
COM573514	"A health trust that posted the private details of 6,574 members of staff on its website".	A.8 Asset management	A.9 Access control	BBC[161]
COM0595607	"A health trust revealed the email addresses of more than 700 users of a HIV service".	A.7 Human Resource Security	A.8 Asset management	BBC[162]

Table 17 Project evaluation of LA ICO CMP data using ISO 27001

ICO Ref	ICO Nature	Annex A Primary	Annex B Secondary	Source
ENF0361170	“Fax error - leading to disclosure of personal data”.	A.8 Asset management	A.16 Information security incident management	BW[163]
ENF0370035	“Theft of unencrypted laptop containing personal data.”.	A.7 Human Resource Security	A.18 Compliance	BW[164]
ENF0370051	“Theft of unencrypted laptop containing personal data.”.	A.12 Operations security	A.18 Compliance	BW[165]
ENF0316728	“Various incidents concerning the disclosure of personal data via email to incorrect recipients”.	A.7 Human Resource Security	A.8 Asset management	BW[166]
ENF0376738	“Various incidents concerning the disclosure of personal data via email to incorrect recipient”.	A.7 Human Resource Security	A.8 Asset management	BW[167]
ENF0379968	“Disclosure of personal data via email to incorrect recipients”.	A.7 Human Resource Security	A.8 Asset management	BW[168]
ENF0397876	“Personal data stolen from a public house”.	A.7 Human Resource Security	A.18 Compliance	BW[169]
ENF0395125	“Personal data hand delivered to incorrect recipient“.	A.7 Human Resource Security	A.18 Compliance	BW[170]
ENF0393688	“Disclosure of personal data via email to unintended recipients”.	A.7 Human Resource Security	A.8 Asset management	BW[171]
ENF0404675	“Case papers containing personal data stolen from staff members house”.	A.8 Asset management	A.18 Compliance	BW[172]

ICO Ref	ICO Nature	Annex A Primary	Annex B Secondary	Source
ENF0415882 & ENF0387535	“Personal data sent in error to incorrect family”.	A.8 Asset management	A.16 Information security incident management	BW[173]
ENF0428682	“Disclosure of personal data via email to incorrect recipient”.	A.7 Human Resource Security	A.8 Asset management	BW[174]
ENF0419390	“Personal data disclosed in error to incorrect recipient”.	A.8 Asset management	A.7 Human Resource Security	BW[175]
ENF0426300	“Personal data disclosed in error to incorrect recipient.	A.8 Asset management	A.7 Human Resource Security	BW[176]
ENF0402909	“Personal data disclosed in error to incorrect recipient”.	A.8 Asset management	A.7 Human Resource Security	BW[177]
ENF0441312	“Personal data left on a train”.	A.7 Human Resource Security	A.18 Compliance	BW[151]
ENF0453668	“Personal data disclosed in error“.	A.8 Asset management	A.18 Compliance	BW[178]
ENF0456704	“Personal details of over 2,000 residents released online via WDTK. website”.	A.8 Asset management	A.7 Human Resource Security	BW[179]
ENF0419022	“Loss of unencrypted memory device containing sensitive personal data”.	A.8 Asset management	A.18 Compliance	BW[180]
COM0595607	“The data controller failed to take appropriate organisational measures against unauthorised processing of personal data”.	A.7 Human Resource Security	A.18 Compliance	BBC[181]

ICO Ref	ICO Nature	Annex A Primary	Annex B Secondary	Source
COM0596385	“The council published personal information about a family in planning application documents which it made publicly available online.”	A.7 Human Resource Security	A.8 Asset management	BBC[182]
COM0557351	“The council were fined by the ICO for leaving personal information vulnerable to attack”.	A.15 Supplier relationships	A.18 Compliance	BBC[183]
ENF0689691	Information about service users published online by the council when seeking companies to apply for care contracts. The service users were identifiable by their address.	A.8 Asset management	A.18 Compliance	ICO[184]
COM0602800	North London council fined after parking ticket system flaw leaves personal information at risk	A.14 System Acquisition, Development and Maintenance	A.18 Compliance	ICO[152]
COM0694273	Unlawfully identified 943 people who owned vacant properties in their borough.	A.7 Human Resource Security	A.18 Compliance	ICO[185]

Appendix C Project Evaluation of ICO Security Incident Data

Table 18 Project evaluation of ICO security incident data 2016/17 and 2017/18

ICO Incident / Breach type;	Assumed Annex A Control Set Failure	2016/17		2017/18	
		NHS	LA	NHS	LA
Cryptographic flaws	A.10 Cryptography	3	0	1	0
Cyber incident – unknown	A.16 Incident Mgmt.	3	0	0	0
Cyber incident (exfiltration)	A.13 Comms. Security	32	1	0	0
Cyber incident (key logging software)	A.12 Operations Sec.	0	0	0	0
Cyber incident (other – DDOS etc.)	A.13 Comms. Security	8	2	3	0
Cyber incident (phishing)	A.7 Human Resource Sec.	2	1	1	0
Cyber security misconfiguration	A.14 System Dev.	10	8	11	3
Data left in insecure location	A.7 Human Resource Sec.	57	6	97	11
Data posted/faxed to incorrect recipient	A.7 Human Resource Sec.	191	56	225	60
Data sent by email to incorrect recipient	A.7 Human Resource Sec.	94	24	162	42
Failure to redact data	A.7 Human Resource Sec.	62	54	62	70
Failure to use bcc when sending email	A.7 Human Resource Sec.	24	12	35	19
Insecure disposal of hardware	A.11 Physical Security	3	1	0	0
Insecure disposal of paperwork	A.11 Physical Security	42	3	23	2
Loss/theft of only copy of encrypted data	A.7 Human Resource Sec.	0	0	2	0
Loss/theft of paperwork	A.7 Human Resource Sec.	166	25	183	41
Loss/theft of unencrypted device	A.7 Human Resource Sec.	29	10	32	3
Verbal disclosure	A.7 Human Resource Sec.	22	8	19	6
Brute Force (Password Attack)	A.9 Access Control	N/A	N/A	0	0
Malware	A.12 Operations Sec.	N/A	N/A	6	1
Ransomware	A.12 Operations Sec.	N/A	N/A	9	0
Unauthorised Access (Cyber)	A.9 Access Control	N/A	N/A	6	1
Blank	Unknown	N/A	N/A	0	2
Other principle 7 failure	Unknown	198	38	286	52
Totals		**946**	**249**	**1163**	**313**