Emerald Information Management and Computer Security

Published incidents and their proportions of human error

Journal:	*Information and Computer Security*
Manuscript ID	ICS-12-2018-0147
Manuscript Type:	Original Article
Keywords:	Information security, incidents, breaches, human error, HEART, GISAT

Published incidents and their proportions of human error

Abstract

Purpose
- The information security field experiences a continuous stream of information security incidents and breaches, which are publicised by the media, public bodies and regulators. Despite the need for information security practices being recognised and in existence for some time the underlying general information security affecting tasks and causes of these incidents and breaches are not consistently understood, particularly with regard to human error.
Methodology
- This paper analyses recent published incidents and breaches to establish the proportions of human error, and where possible subsequently utilises the HEART human reliability analysis technique, which is established within the safety field.
Findings
- This analysis provides an understanding of the proportions of incidents and breaches that relate to human error as well as the common types of tasks that result in these incidents and breaches through adoption of methods applied within the safety field.
Originality
- This research provides original contribution to knowledge through the analysis of recent public sector information security incidents and breaches in order to understand the proportions that relate to human error.

Keywords

Information security, incidents, breaches, human error, HEART, GISAT

1. Introduction

Our previous work (Evans, He, Yevseyeva, *et al.*, 2018) analysed data breach trends published in 2017 that were reported to the UK Information Commissioner's Office (Information Commissioner's Office, 2018) and identified that a number of UK sectors have experienced significant increases in reported information security incidents in Q4 2017. In some sectors such as the health sector this is primarily due to incidents that relate to people and human error. Despite this, the information security community does not have a thorough understanding of what constitutes a human error and often resorts to general basic awareness or training on information security following an incident rather than dealing with the causal factors (Mahfuth *et al.*, 2017). Current practices fall regularly short of identifying the actual root cause of human error related information security incidents even though people are recognized as being the weakest link in information security controls (Metalidou *et al.*, 2014; Halevi *et al.*, 2017; Mahfuth *et al.*, 2017; Parsons *et al.*, 2017; Furnell *et al.*, 2018). There are also no established human error information security frameworks in practice to enable not only effective resolution of human error related information security incidents but also the prevention of these events.

The aim and motivation for this research is to analyse and establish the volumes and causes of information security incidents and breaches, published by the Information Commissioner's Office (ICO) and the UK National Health Service (NHS), that relate to human error for the periods of Q1 and Q2 2018. Where sufficient data has been published, incidents are mapped to the established Human Error Assessment and Reduction Technique (HEART) human reliability analysis method, which is widely utilised within the safety field, to understand the types and context of tasks which are associated with the published incidents and breaches.

This research provides original contribution to knowledge through the analysis of recent public sector information security incidents in order to understand the proportions that relate to human error as well as the common generic task types (GTT), as defined within the HEART (Williams, 1992) technique, and general information security affecting tasks (GISAT) (Evans, Maglaras, *et al.*, 2018) that lead to these events. The research also supports the applicability of the HEART human reliability analysis technique within the information security field.

The remainder of paper is structured as follows. Section 2 presents related research into the human factor of information security. Section 3 provides an overview of the method applied for the research into published information security incidents and breaches and section 4 presents the results of the research. Section 5 delivers the key findings and section 6 concludes the research and outlines future work.

2. Related Work

There have been many research articles published on the topic of information security but proportionally very few articles dedicated to the human factor and specifically human error. In our previous research (Evans *et al.*, 2016) we emphasised this gap in current research and also emphasised the need for empirical research into human error effects on information security assurance to understand the underlying causes of human error. Human error is defined as non-deliberate, unintentional or accidental cause of poor information security (Werlinger, Hawkey and Beznosov, 2009). Amongst published articles human error is identified as being associated with a large proportion of information security incidents or breaches (Komatsu, Takagi and Takemura, 2013; Stewart and Jürjens, 2017) and the most critical factor in the management of information security (Stewart and Jürjens, 2017). Literature has consistently presented that effective information security management must essentially embrace the human factor in addition to technology (Werlinger, Hawkey and Beznosov, 2009; Asai and Hakizabera, 2010; Frangopoulos, Eloff and Venter, 2014; Stewart and Jürjens, 2017, Hadlington et al 2019) and that the security of IT systems and platforms have been undermined by human failings (Lacey, 2010).

It is widely accepted that security incidents related to human perpetrators from internal sources are the most difficult to prevent (Hwang *et al.*, 2017) and not an easy task (McLeod and Dolezel, 2018). A fundamental challenge in complex sociotechnical systems is that of relying upon humans to achieve reliable operations (Kyriakidis *et al.*, 2018) and it is difficult to integrate the human factor in to a plan-do-check-act cycle of an effective Information Security Management System (ISMS) (Frangopoulos, Eloff and Venter, 2014). Addressing these difficulties requires new interventions to change human awareness, attitudes and behaviour (Lacey, 2010). To this point, Stewart (Stewart and Jürjens, 2017) presented in his work that human issues were the main issues of the bank he was engaged with. Incidents where organisational insiders disclose sensitive information can have a severe impact on an organisation and are challenging to understand and implement effective controls (Choi, Martins and Bernik, 2018) due to the complexity of human behaviour (Nguyen *et al.*, 2018).

Human error quantification has varied in published literature. Frangopoulos et al (Komatsu, Takagi and Takemura, 2013) presented that 42 percent of security incidents resulted from human error whereas Stewart (Stewart and Jürjens, 2017) stated that 65 percent were due to some forms of human error. Alavi et al (Alavi, Islam and Mouratidis, 2016) presented research, which found that 64 percent of security incidents were directly related to human error. Whereas Asai and Hakizabera (Asai and Hakizabera, 2010) stated in their research that 80 percent of information security breaches are caused by human error. The information security field should study methods used within the safety field (Lacey, 2010), where it was found that 90 percent of accidents were caused by human failure. It was also suggested that new interventions are required to change human behaviour (Lacey, 2010) and that few information security practitioners have an understanding of proven methodologies for changing human behaviour. It was also stated that factors such as stress, lack of training or supervision, and bad system or process design are the underlying causes of breaches (Lacey, 2010) and also that information security management remains relatively weak in conducting root cause analysis of minor incidents.

The information security risk management approach is useful for maintaining acceptable risk levels, but they are not developed to solve complex socio-technical problems (Wangen *et al.*, 2017). In fact despite it being recognised that the actions and behaviour of organisational insiders are essential to achieve information security success, the human factor is often overlooked (Choi, Martins and Bernik, 2018). Methods and techniques to perform root cause analysis and risk assessment to identify the factors that enable the early detection of danger exist and have been shown to give reliable results even when highly complex human factors aspects are involved (Cacciabue and Vella, 2010). It has been published that insights from root cause analysis are not likely to inform practice or process improvements and it is suggested that there is more human factors and independence undertaken as part of investigations (Hibbert *et al.*, 2018) as long as standardised and explicit processes and techniques are used (National Patient Safety Foundation, 2015). Mayer, Kunz, and Volkamer (Mayer, Kunz and Volkamer, 2017) stated that there a low number of studies investigating behavioural factors of information security and that further literature would be a valuable addition. According to Williams (Williams, 2015) one of the last remaining hurdles to be overcome in the design of safe, reliable systems is the human being as recognised by safety and reliability engineers. Lacey (Lacey, 2010) suggests that Security Managers could benefit from studying the lessons learned in the safety field and He and Johnson (He and Johnson, 2015) presented in their research that the reoccurrence of past security incidents in healthcare showed that lessons had not been learned across healthcare organisations. With regard to risk analysis performed within IT security and the safety field the only main difference is the terminology so it is suggested that IT security is treated the same as systematic failures in the safety field (Braband and Schäbe, 2016).

The healthcare sector continues to be affected by the largest percentage of data breaches (He and Johnson, 2015) with almost two breaches per day being recorded in 2015, which is ten times the volume reported in 2009 presenting a position whereby preventing healthcare breaches is very difficult (McLeod and Dolezel, 2018). The reporting of incidents is core requirement for UK National Health Service (NHS) organisations (Rooksby, Gerry and Smith, 2007). Healthcare breaches have the potential to result in theft, modification or misuse of personal data and healthcare organisations. Processing personal data for health purposes have a legal and moral duty to proactively understand the causes of data breaches as they remain vulnerable to a wide range of threats including human issues (McLeod and Dolezel, 2018).

3. Method

The method employed by this research was to understand the proportions of human error related incidents from published public sector incidents and personal data breaches by the UK Information Commissioner's Office (ICO) and the UK National Health Service (NHS). As there is greater incident detail published for the NHS personal data breaches we were able to use a set of GISATs to map the breaches to, in order to provide a richer level of understanding regarding the specific tasks that were being performed when the incident occurred. Once the GISATs were established we were subsequently able to map the breaches to the HEART GTTs.

HEART was initially published in 1985 and used by numerous organisations and sectors as a mechanism to address the issue of human reliability (Williams, 1992). HEART has been widely used in industry, primarily the nuclear industry (Lyons *et al.*, 2004; Chandler *et al.*, 2006). A detailed HEART user manual (Williams, 1992) was written in 1992 for Nuclear Electric plc, now EDF Energy. The HEART method comprises of a set of 9 GTTs as shown in Table 1 with associated nominal human unreliability and upper bounds and also 38 error producing conditions (EPC) and their accompanying strength values. The GTTs are a core component of the HEART technique which looks to match the task under consideration with a predefined list of task descriptions.

A	Totally unfamiliar task, performed at speed with no real idea of the likely consequences of actions taken.
B	Shift or restore system to a new or original state at a single attempt without supervision or procedures.
C	Complex task requiring a high level of understanding and skill.
D	Fairly simple task performed rapidly or given insufficient or inadequate attention.
E	Routine, highly-practiced, rapid task involving relatively low level of skill.
F	Restore or shift a system to original or new state following procedures, with some checking.
G	Completely familiar, well designed, highly practiced routine task occurring several times per hour, performed to highest possible standards by highly motivated, highly trained and experienced persons, totally aware of implications of failure, with time to correct potential error, but without the benefit of significant job aids.
H	Respond correctly to system command even when there is an assisting or automated supervisory system providing accurate interpretation of system state.
M	Miscellaneous task for which no description can be found.

Table 1 – HEART GTTs (Williams, 1992)

The Q1 and Q2 2018 incident trends published by the ICO (Information Commissioner's Office, 2018) were analysed to ascertain a greater degree of understanding of the proportions of human error related information security incidents. In addition to analysis of the ICO data, security trend analysis was also performed on the published NHS serious incidents requiring investigation (SIRI) level 2 incidents relating to Q1 and Q2 (NHS Digital, 2018). Further analysis of the incidents was conducted by mapping each of the human error related SIRI level 2 incidents to a set of General Information Security Affecting Tasks (GISAT), which subsequently enabled the mapping to the HEART GTTs. The GISATs were developed during our wider research and empirical feasibility study into 12 months of reported information security incidents within public and private sector organisations (Evans, He, Maglaras, *et al.*, 2018; Evans, Maglaras, *et al.*, 2018).

The primary focus of this research was public sector incidents and breaches but also undertook analysis of combined data for all sectors, including private sector, to enable a holistic set of results. In order to enable the analysis to be performed and establish which incidents were likely, possibly or unlikely related to human error, we developed a mapping based upon the analysis of the published incidents and experience gained through associated empirical research (Evans, He, Maglaras, *et al.*, 2018; Evans, Maglaras, *et al.*, 2018). These mappings required updating following our previous publication (Evans, He, Yevseyeva, *et al.*, 2018) as the ICO incident/breach types were changed at source (Information Commissioner's Office, 2018) which is presented below. The ICO has replaced the initial incident/breach types and created new ones that are higher-level in terms of information security, such as disclosure of data, and also cover specific data protection elements such as the right to prevent processing. Our mapping update pertained to the adding of the new ICO incident/breach type, mapping to the previous ICO incident/breach type and capturing the new human error likelihood. This modification enabled comparisons with previous results (Evans, He, Yevseyeva, *et al.*, 2018) to be undertaken to establish if the results were consistent in terms of the proportions of human error. In addition we also mapped the new ICO incident/breach types to the principles of confidentiality, integrity and availability as outlined within the ISO27001 standard (The British Standards Institution, 2013).

New ICO Incident / Breach Type	**Confidentiality**	**Integrity**	**Availability**	**Human Error Likelihood**	**Previous ICO Incident / Breach Type** (Information Commissioner's Office, 2018)	**Previous ICO Incident / Breach Type Human Error Likelihood** (Evans, He, Yevseyeva, *et al.*, 2018)	**Rationale**
Disclosure of data	Y			Likely	Data posted/ faxed to incorrect recipient	Likely	The data would likely be posted or faxed to the wrong recipient unintentionally
					Data sent by email to incorrect recipient	Likely	The data would likely be emailed to the wrong recipient unintentionally
					Failure to use bcc when sending email	Likely	The failure to use bcc would likely be unintentional
					Verbal disclosure	Likely	The data would likely be disclosed by a person unintentionally

New ICO Incident / Breach Type	**Confidentiality**	**Integrity**	**Availability**	**Human Error Likelihood**	**Previous ICO Incident / Breach Type** (Information Commissioner's Office, 2018)	**Previous ICO Incident / Breach Type Human Error Likelihood** (Evans, He, Yevseyeva, *et al.*, 2018)	**Rationale**
Excessive / Irrelevant data	Y	Y		Likely	Failure to redact data	Likely	The data would likely be redacted unintentionally
Fair processing info not provided		Y	Y	Possibly	n/a	n/a	The failure to provide fair processing info could be organisational or possibly human error
Inaccurate data		Y		Likely	n/a	n/a	The inaccurate data would likely be captured or edited unintentionally
Obtaining data	Y			Possibly	n/a	n/a	The non-compliant obtaining of data could be organisational or possibly human error
Retention of data			Y	Possibly	n/a	n/a	The non-compliant retention of data could be organisational or possibly human error
S170	Y			Unlikely	n/a	n/a	The unlawful obtaining of data, where the victim is likely to be the data controller, is unlikely to be unintentional human error.

New ICO Incident / Breach Type	**Confidentiality**	**Integrity**	**Availability**	**Human Error Likelihood**	**Previous ICO Incident / Breach Type** (Information Commissioner's Office, 2018)	**Previous ICO Incident / Breach Type Human Error Likelihood** (Evans, He, Yevseyeva, *et al.*, 2018)	**Rationale**
Right to prevent processing	Y			Unlikely	n/a	n/a	The right to prevent processing is likely to be an organisational non-compliance rather than human error.
Security	Y	Y	Y	Possibly	Data left in insecure location	Likely	The data would likely be left by a person unintentionally
					Insecure disposal of hardware	Possibly	The insecure disposal of hardware could be technical, procedural or possibly human error
					Insecure disposal of paperwork	Possibly	The insecure disposal of paperwork could be technical, procedural or possibly human error
					Loss/theft of only copy of encrypted data	Possibly	The category covers both loss of equipment ,which is likely to be unintentional human error, but also mainly theft of equipment which is unlikely to be human error

New ICO Incident / Breach Type	**Confidentiality**	**Integrity**	**Availability**	**Human Error Likelihood**	**Previous ICO Incident / Breach Type** (Information Commissioner's Office, 2018)	**Previous ICO Incident / Breach Type Human Error Likelihood** (Evans, He, Yevseyeva, *et al.*, 2018)	**Rationale**
					Loss/theft of paperwork	Likely	The category covers both mainly loss of paperwork which is likely to be unintentional human error but also infrequent theft of paperwork which is unlikely to be human error
					Loss/theft of unencrypted device	Possibly	The category covers both loss of equipment, which is likely to be unintentional human error, but also mainly theft of equipment which is unlikely to be human error
					Other principle 7 failure	Possibly	This is a broad category and incidents could possibly be as a result of unintentional human error
Subject access	Y	Y	Y	Possibly	n/a	n/a	The failure to process a subject access request in a compliant manner could possibly be human error

New ICO Incident / Breach Type	Confidentiality	Integrity	Availability	Human Error Likelihood	Previous ICO Incident / Breach Type (Information Commissioner's Office, 2018)	Previous ICO Incident / Breach Type Human Error Likelihood (Evans, He, Yevseyeva, *et al.*, 2018)	Rationale
Unable to identify	Y	Y	Y	Possibly	n/a	n/a	This is a broad category which could possibly be as a result of human error
Use of data	Y	Y	Y	Possibly	n/a	n/a	The use of data in a non-compliant manner could be organisational or possibly human error
Not specified	Y	Y	Y	Possibly	n/a	n/a	This is a broad category which could possibly be as a result of human error

Table 2 – Mapping of ICO data security incident categories to human error likelihood

This study analysed 7202 incidents published by the ICO (Information Commissioner's Office, 2018) and 60 NHS SIRI incidents (NHS Digital, 2018). The development of the mapping between incident/breach types and the human error likelihood as shown in Table 2 was established by the authors of this paper based upon professional experience and the completion of feasibility studies which form part of the wider research programme (Evans, He, Maglaras, *et al.*, 2018; Evans, Maglaras, *et al.*, 2018). The mapping of the ICO data was undertaken by aligning each of the ICO incident/breach type to a likelihood. The analysis of the NHS data, which contained basic details of each incident, was undertaken by initially establishing if human error was a reason for the incident occurring or not, mapping each incident to a GISAT and subsequently mapping to a HEART GTT to establish the most common tasks associated with the incidents. We were unable to map the ICO incident/breach types to the HEART GTTs as the ICO data only provided volumes for each category with no specific information for each incident.

4. Results

The results of the analysis of the published public sector (Central and Local Government and Health) personal data breaches and NHS SIRI level 2 incidents are presented in the tables and figures below.

The analysis of 7202 published personal data breaches by the ICO for all sectors can be shown in Table 3 and Figure 1. It was established that 64% of the incidents were likely to be as a result of human error and that a further 35% could possibly be as a result of human error. Therefore, combining both categories provides a view that 97% of all personal data breaches reported to the ICO could have been as a result of human error.

All Sectors		
Human Error Likelihood	**Count**	**Percentage**
Likely	4641	64.44
Possibly	2531	35.14
Unlikely	30	0.41

Table 3 – Human error likelihood of ICO data security incident trends for all sectors

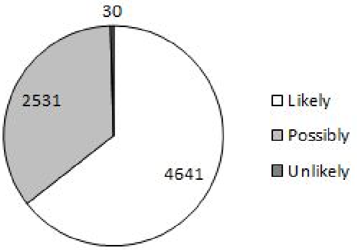

Figure 1 – Likelihood of human error ICO data security incident trends for all sectors

The analysis was also performed on specific central government (Table 4 and Figure 2), local government (Table 5 and Figure 3) and health sectors (Table 6 and Figure 4). The analysis found that incidents were likely to relate to human error for these three sectors between 67% and 77%. However, taking into account the possible human errors the percentages increased significantly. This accumulation found that data security incidents relating to human error was possibly 99% for central government, local government and health sectors.

Central Government Sector		
Human Error Likelihood	**Count**	**Percentage**
Likely	95	67.37
Possibly	45	31.91
Unlikely	1	0.71

Table 4 – Human error likelihood of ICO data security incident trends for central government

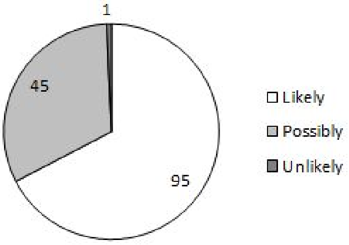

Figure 2 – Likelihood of human error ICO data security incident trends for central government

Local Government Sector		
Human Error Likelihood	**Count**	**Percentage**
Likely	433	76.91
Possibly	127	22.55
Unlikely	3	0.53

Table 5 – Human error likelihood of ICO data security incident trends for local government

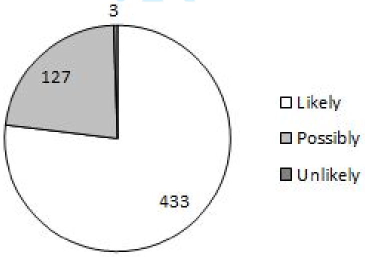

Figure 3 – Likelihood of human error ICO data security incident trends for local government

Health Sector		
Human Error Likelihood	**Count**	**Percentage**
Likely	887	68.44
Possibly	404	31.17
Unlikely	5	0.38

Table 6 – Human error likelihood of ICO data security incident trends for health

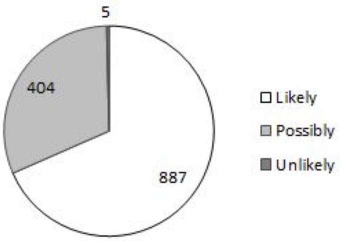

Figure 4 – Likelihood of human error ICO data security incident trends for health

Each of the reported NHS SIRI incidents and associated details were analysed and it was identified that 40 (67%) of the most serious NHS personal data security incidents pertained to human error.

SIRI Level 2 Incidents		
Human Error	**Count**	**Percentage**
Yes	40	67
No	20	33

Table 7 – NHS SIRI level 2 incidents

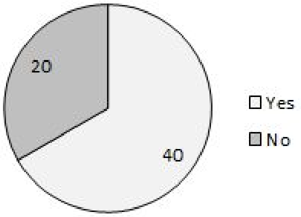

Figure 5 – Proportion of human error for NHS SIRI 2 incidents

In addition, 883 of the 1296 incidents related to disclosure of data which mapped to the confidentiality principle indicating that this is the most impacted principle with regard to human error related incidents.

This analysis of the Q1 and Q2 2018 NHS SIRI level 2 incidents found that 11 (28%) were posting an item or information, 11 (28%) were safeguarding information or equipment, and 8 (20%) were sending an email. We were able to manually map each incident to the list of GISATs using the rich details published for each incident by the NHS. The details of this granular analysis and mapping to GISATs can be seen in Table 8 and Figure 6.

General Information Security Affecting Tasks (GISAT)	Count	Percentage of human error incidents	HEART GTT
GISAT1- Sending an email	8	20	G
GISAT2 - Entering, updating or deleting data within a system, file or document	5	13	D
GISAT3 - Posting an item or information	11	28	E

General Information Security Affecting Tasks (GISAT)	Count	Percentage of human error incidents	HEART GTT
GISAT4 - Configuring a system	1	3	B
GISAT5 - Administering a system	0	0	D
GISAT6 - Scanning a document	0	0	D
GISAT7 - Printing a document	1	3	D
GISAT8 - Providing information verbally	0	0	G
GISAT9 - Delivering information or equipment	1	3	G
GISAT10 - Filing or sorting information	0	0	G
GISAT11 - Reading or checking an email, file, document or item	0	0	G
GISAT12 - Safeguarding information or equipment	11	28	G
GISAT13 – Destroying information or equipment	0	0	D
GISAT14 – Accessing a location or environment	0	0	G
GISAT15 - Faxing information	0	0	D
GISAT16 - Sharing or handing over information or equipment in person	2	5	G

Table 8 - Mapping of NHS SIRI 2 incidents to GISATs and association with HEART GTTs

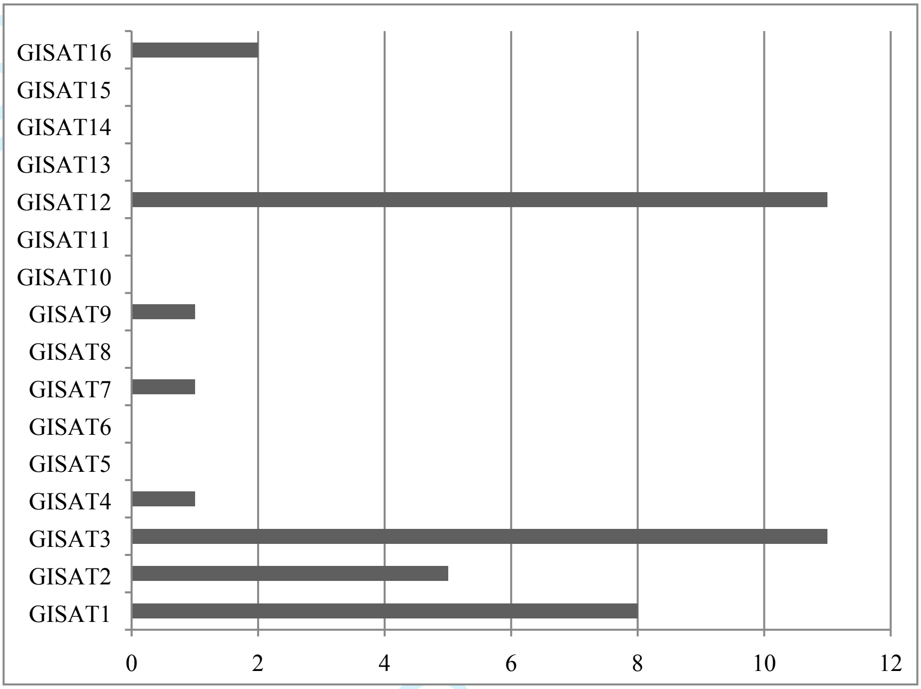

Figure 6 - Mapping of NHS SIRI 2 incidents to GISATs

Once the NHS SIRI level 2 incidents had been mapped to the GISATs it was possible to create a conceptual mapping to the HEART GTTs. The mapping can be seen in Table 8. In addition the volumes of each selected GTTs that have been mapped to the Q1 and Q2 2018 SIRI level 2 incidents can be seen below. It was established that none of the published incidents were able to be mapped to GTTs A, C, E, F, H or M.

GTT	Count	Percentage
B	1	2.5
D	6	15
E	11	27.5
G	22	55

Table 9 – HEART GTT mapping to NHS SIRI level 2 incidents

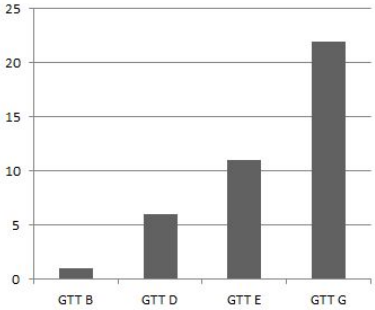

Figure 7 – HEART GTT mapping to NHS SIRI level 2 incidents

In addition, 100% (40) of the human error-related incidents mapped to the confidentiality principle again indicating that this is the most impacted principle with regard to human error related incidents. 23 of the 40 human error-related incidents also mapped to the availability principle and 8 incidents were able to be mapped to the integrity principle.

5. Discussion

Following analysis of the published ICO data it was identified that 64% of reported incidents across all sectors were likely to be the result of human error, which aligns to the research published by (Alavi, Islam and Mouratidis, 2016; Stewart and Jürjens, 2017) and matches our analysis undertaken on 2017 data (Evans, He, Yevseyeva, *et al.*, 2018). In addition a further 35% could also possibly be as a result of human error. Therefore, the analysis found that 99% of data security incidents reported to the ICO could possibly have been as a result of human error suggesting actual rates of human error related information security incidents is higher than currently understood by the information security community. These high volumes of possible human error information security incidents align to the proportions of human failure that led to accidents in the safety field (Lacey, 2010). This supports the view that the established root cause methods utilised within the safety field would demonstrate a higher proportion of human error behind current information security incident and breach events than currently recognised.

Each of the 60 reported NHS SIRI level 2 incidents and associated details were analysed and it was identified that 40 (67%) of the most serious NHS personal data security incidents pertained to human error which again aligns to published research (Alavi, Islam and Mouratidis, 2016).

Following analysis of the published NHS SIRI level 2 incidents it was identified that the most common general information security affecting tasks were postage of information and safeguarding of information or equipment. They were followed by the use of email showing that focus should be applied to external sharing and communication of information. The analysis of the same incidents against the HEART GTTs found that the most common generic task type associated with information security incidents is a completely familiar routine task.

Analysis of both NHS and ICO data showed that the confidentiality principle was the most common principle for all human error-related information security incidents compared to integrity or availability.

6. Conclusions and Future Work

In conclusion, it has been identified that the actual volumes of personal data breaches and information security incidents are greater than currently understood by the information security community. Therefore, in order to reduce the volumes of breaches and incidents the information security field should understand the human reliability analysis techniques applied within the safety field. The application, and adaptation, of methods used within the safety field will enable the underlying root causes of human error to be understood and acted upon, which will reduce future volumes of information security incidents and breaches. In addition, organisations should focus on routine operational tasks performed by employees that involve the external sharing or communication of confidential or personal data.

The results of this work supports our previous analysis of 2017 data (Evans, He, Yevseyeva, *et al.*, 2018) and feasibility studies (Evans, He, Maglaras, *et al.*, 2018; Evans, Maglaras, *et al.*, 2018) showing a consistent view with regard to the proportions of information security incidents and breaches caused by human error. This research provides original contribution to knowledge through the analysis of recent, Q1 and Q2 2018, information security incidents and breaches in addition to our previous similar study of ICO and NHS incidents that were published (Evans, He, Yevseyeva, *et al.*, 2018). This study clearly provides an understanding of the proportions of incidents that relate to human error and confirms previously obtained results. In addition, it demonstrates the most common generic task types (GTT), as defined within the HEART (Williams, 1992) technique, and general information security affecting tasks (GISAT) (Evans, Maglaras, *et al.*, 2018) that lead to these incidents/breaches. The research also reinforces both the need and applicability of human reliability analysis techniques such as IS-CHEC (Evans, He, Maglaras, *et al.*, 2018) to be utilised within the information security field in order to address the most common incident types and reduce their current volumes.

We will be continuing our research into the feasibility of human reliability analysis within the information security field including publishing associated 12 months real-time incident studies, which have been undertaken within public and private sector organisations. In addition, HEART will be subject to further adaptation to produce an empirically validated Information Security Core Human Error Causes (IS-CHEC) product, which will be developed as a key element of the ongoing action research.

7. References

Alavi, R., Islam, S. and Mouratidis, H. (2016) 'An information security risk-driven investment model for analysing human factors', *Information and Computer Security*. Emerald Group Publishing Limited , 24(2), pp. 205–227. doi: 10.1108/ICS-01-2016-0006.

Asai, T. and Hakizabera, A. U. (2010) 'Human-related problems of information security in East African cross-cultural environments', *Information Management & Computer Security*. Edited by S. M. Furnell. Emerald Group Publishing Limited, 18(5), pp. 328–338. doi: 10.1108/09685221011095245.

Braband, J. and Schäbe, H. (2016) 'Probability and security – pitfalls and chances', *Safety and Reliability*. Taylor & Francis, 36(1), pp. 3–12. doi: 10.1080/09617353.2016.1148920.

Cacciabue, P. C. and Vella, G. (2010) 'Human factors engineering in healthcare systems: The problem of human error and accident management', *International Journal of Medical Informatics*. Elsevier, 79(4), pp. e1–e17. doi: 10.1016/J.IJMEDINF.2008.10.005.

Chandler, T. *et al.* (2006) 'Human Reliability Analysis Methods Selection Guidance for NASA', *National Aeronautics and Space Administration*, (July), p. 175. Available at: http://www.hq.nasa.gov/office/codeq/rm/docs/HRA_Report.pdf.

Choi, S., Martins, J. T. and Bernik, I. (2018) 'Information security: Listening to the perspective of organisational insiders', *Journal of Information Science*. SAGE Publications Ltd, p. 016555151774828. doi: 10.1177/0165551517748288.

Evans, M. *et al.* (2016) 'Human behaviour as an aspect of cybersecurity assurance', *Security and Communication Networks*, 9(17), pp. 4667–4679. doi: 10.1002/sec.1657.

Evans, M., He, Y., Yevseyeva, I., *et al.* (2018) 'Analysis of published public sector information security incidents and breaches to establish the proportions of human error', in

Proceedings of the 12th International Conference on the Human Aspects of Informarion Security Assurance - HAISA 2018, pp. 911–921.

Evans, M., He, Y., Maglaras, L., *et al.* (2018) ‘Core Human Error Causes (IS-CHEC) Technique in Public Sector and Comparison with the Private Sector’, *International Journal of Medical Informatics*, Submitted.

Evans, M., Maglaras, L., *et al.* (2018) ‘HEART-IS: A Novel Technique fro Evaluating Human Error-Related Information Security Incidents’, *Computers & Security*. Elsevier Advanced Technology, Accepted.

Frangopoulos, E. D., Eloff, M. M. and Venter, L. M. (2014) ‘Human Aspects of Information Assurance: A Questionnaire-based Quantitative Approach to Assessment’. Available at: https://pdfs.semanticscholar.org/8d43/bcc32ddaa0bfd067d822997018154e435a4f.pdf (Accessed: 26 May 2018).

Furnell, S. *et al.* (2018) ‘Enhancing security behaviour by supporting the user’, *Computers & Security*. Elsevier Ltd, 75, pp. 1–9. doi: 10.1016/j.cose.2018.01.016.

Halevi, T. *et al.* (2017) ‘Cultural and psychological factors in cyber-security’, *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services*. Rinton Press Inc., 13(1–2), pp. 43–56. Available at: https://www.scopus.com/record/display.uri?eid=2-s2.0-85038911760&origin=resultslist&sort=plf-f&src=s&st1=Cultural+and+Psychological+Factors+in+Cyber-Security&st2=&sid=dc07e210e92cb781fbb49da710eb35c4&sot=b&sdt=b&sl=67&s=TITLE-ABS-KEY%28Cultural+and+Psycho (Accessed: 17 March 2018).

He, Y. and Johnson, C. (2015) ‘Improving the redistribution of the security lessons in healthcare: An evaluation of the Generic Security Template’, *International Journal of Medical Informatics*. Elsevier, 84(11), pp. 941–949. doi: 10.1016/J.IJMEDINF.2015.08.010.

Hibbert, P. D. *et al.* (2018) ‘Are root cause analyses recommendations effective and sustainable? An observational study’, *International Journal for Quality in Health Care*. Oxford University Press, 30(2), pp. 124–131. doi: 10.1093/intqhc/mzx181.

Hwang, I. *et al.* (2017) ‘Why not comply with information security? An empirical approach for the causes of non-compliance’, *Online Information Review*. Emerald Publishing Limited , 41(1), pp. 2–18. doi: 10.1108/OIR-11-2015-0358.

Information Commissioner’s Office (2018) *Data security incident trends*. Available at: https://ico.org.uk/action-weve-taken/data-security-incident-trends/.

Komatsu, A., Takagi, D. and Takemura, T. (2013) ‘Human aspects of information security’, *Information Management & Computer Security*. Edited by S. M. Furnell. Emerald Group Publishing Limited, 21(1), pp. 5–15. doi: 10.1108/09685221311314383.

Kyriakidis, M. *et al.* (2018) ‘Understanding human performance in sociotechnical systems – Steps towards a generic framework’, *Safety Science*. Elsevier, 107, pp. 202–215. doi: 10.1016/J.SSCI.2017.07.008.

Lacey, D. (2010) ‘Understanding and transforming organizational security culture’, *Information Management & Computer Security*. Edited by S. M. Furnell. Emerald Group Publishing Limited, 18(1), pp. 4–13. doi: 10.1108/09685221011035223.

Lyons, M. *et al.* (2004) ‘Human reliability analysis in healthcare : A review of techniques’, *International Journal of Risk & Safety in Medicine*. IOS Press, 16, pp. 223–237. Available at: https://www.researchgate.net/profile/Maria_Woloshynowych/publication/228888804_Human_reliability_analysis_in_healthcare_A_review_of_techniques/links/00b7d532c94fc43200000000/Human-reliability-analysis-in-healthcare-A-review-of-techniques.pdf.

Mahfuth, A. *et al.* (2017) ‘A systematic literature review: Information security culture’, in *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*. IEEE, pp. 1–6. doi: 10.1109/ICRIIS.2017.8002442.

Mayer, P., Kunz, A. and Volkamer, M. (2017) ‘Reliable Behavioural Factors in the Information Security Context’, in *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES ’17*. New York, New York, USA: ACM Press, pp. 1–10. doi: 10.1145/3098954.3098986.

McLeod, A. and Dolezel, D. (2018) ‘Cyber-analytics: Modeling factors associated with healthcare data breaches’, *Decision Support Systems*. North-Holland, 108, pp. 57–68. doi: 10.1016/J.DSS.2018.02.007.

Metalidou, E. *et al.* (2014) ‘The Human Factor of Information Security: Unintentional Damage Perspective’, *Procedia - Social and Behavioral Sciences*. Elsevier, 147, pp. 424–428. doi: 10.1016/J.SBSPRO.2014.07.133.

National Patient Safety Foundation (2015) ‘RCA Improving Root Cause Analyses and Actions to Prevent Harm’, *Www.Npsf.Org*, (January), p. 51. Available at: https://scholar.google.co.uk/scholar?hl=en&as_sdt=0%2C5&q=RCA2+Improving+Root+cause+Analyses+and+Actions+to+prevent+harm&btnG= (Accessed: 11 November 2018).

Nguyen, P. H. *et al.* (2018) ‘Understanding User Behaviour through Action Sequences: from the Usual to the Unusual’, *IEEE Transactions on Visualization and Computer Graphics*, pp. 1–1. doi: 10.1109/TVCG.2018.2859969.

NHS Digital (2018) *Information Governance Incidents Closed*. Available at: https://www.igt.hscic.gov.uk/resources/IGIncidentsPublicationStatement.pdf. (Accessed: 14 December 2018).

Parsons, K. *et al.* (2017) ‘The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies’, *Computers & Security*. Elsevier Ltd, 66, pp. 40–51. doi: 10.1016/j.cose.2017.01.004.

Rooksby, J., Gerry, R. M. and Smith, A. F. (2007) ‘Incident reporting schemes and the need for a good story’, *International Journal of Medical Informatics*. Elsevier, 76, pp. S205–S211. doi: 10.1016/J.IJMEDINF.2006.05.019.

Stewart, H. and Jürjens, J. (2017) ‘Information security management and the human aspect in organizations’, *Information and Computer Security*. Emerald Publishing Limited , 25(5), pp. 494–534. doi: 10.1108/ICS-07-2016-0054.

The British Standards Institution (2013) *ISO/IEC 27001 - Information security management systems — Requirements*. BSI. Available at: https://shop.bsigroup.com/ProductDetail?pid=000000000030347472&utm_source=google&utm_medium=cpc&utm_campaign=SM-STAN-PRM-CSR-iso27001-1810&creative=307410444133&keyword=%2Biso %2B27001&matchtype=b&network=g&device=c&gclid=EAIaIQobChMI1ovTo7_A3wIVLrvtCh0xi (Accessed: 27 December 2018).

Wangen, G. B. *et al.* (2017) *An Empirical Study of Root-Cause Analysis in Information Security Management Implementation of Information Security Management System and Risk Management View project An Empirical Study of Root-Cause Analysis in Information Security Management*. Available at: https://www.researchgate.net/publication/319753715 (Accessed: 11 November 2018).

Werlinger, R., Hawkey, K. and Beznosov, K. (2009) 'An integrated view of human, organizational, and technological challenges of IT security management', *Information Management & Computer Security*. Edited by S. M. Furnell. Emerald Group Publishing Limited, 17(1), pp. 4–19. doi: 10.1108/09685220910944722.

Williams, J. C. (1992) 'A User Manual for the HEART Human Reliability Assessment Method'. DNV Technica.

Williams, J. C. (2015) 'Heart—A Proposed Method for Achieving High Reliability in Process Operation by Means of Human Factors Engineering Technology', *Safety and Reliability*. Taylor & Francis, 35(3), pp. 5–25. doi: 10.1080/09617353.2015.11691046.