Analysis of published public sector information security incidents and breaches to establish the proportions of human error

M. Evans, Y. He, I. Yevseyeva and H. Janicke,

Cyber Security Centre, De Montfort University, England

e-mail: mark.evans4@my365.dmu.ac.uk; ying.he@dmu.ac.uk; iryna@dmu.ac.uk; heljanic@dmu.ac.uk

Abstract

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. 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. 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.

Keywords

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

1. Introduction

The ICO data security incident trends (Information Commissioner's Office, 2017) shows 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 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 (Furnell et al., 2018; Halevi et al., 2017; Mahfuth et al., 2017; Metalidou et al., 2014; Parsons et al., 2017). 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 motivation for this research is to establish the volumes and causes of publicised information security incidents and breaches that relate to human error and where possible map to the established Human Error Assessment and Reduction Technique (HEART) human reliability analysis method, which is widely utilised within the safety field.

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 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 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 et al., 2009). Amongst published articles human error is identified as being associated with a large proportion of information security incidents or breaches (Komatsu et al., 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 (Asai and Hakizabera, 2010; Frangopoulos et al., 2014; Stewart and Jürjens, 2017; Werlinger et al., 2009) and that the security of IT systems and platforms have been undermined by human failings (Lacey, 2010).

Human error quantification has varied in published literature. Frangopoulos et al (Komatsu et al., 2013) presented that 42 percent of security incidents resulted from human error whereas Stewart (Stewart and Jürjens, 2017) stated 65 percent were due to some forms of human error. Alavi et al (Alavi et al., 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 presented 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.

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 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 (Chandler et al., 2006; Lyons et al., 2004). 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 Q4 2017 incident trends published by the ICO (Information Commissioner's Office, 2017) 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 Q3 2017 (Department of Health, 2017). Further analysis of the incidents was conducted by mapping each of the 124 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.

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 the mapping below based upon analysis of the published incidents.

Category	Human Error Likelihood	Rationale
Data left in insecure location	Likely	The data would likely be left by a person unintentionally
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 redact data	Likely	The data would likely be redacted unintentionally
Failure to use bcc when sending email	Likely	The failure to use bcc would likely be unintentional
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
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
Verbal disclosure	Likely	The data would likely be disclosed by a person unintentionally
Cyber incidents	Unlikely	The cyber incident category tends to relate to malicious or intentional acts so is unlikely to be human error

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

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 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 27% could possibly be as a result of human error. Therefore, combining both categories provides a view that 91% 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	521	63.92
Possibly	220	26.99
Unlikely	74	9.07

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

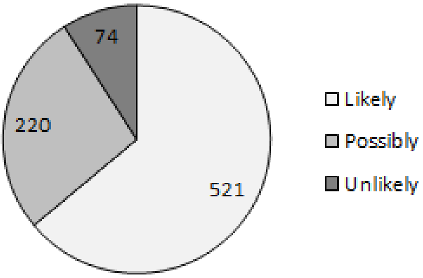

Figure 1 – Likelihood of human error ICO data security incident trends for all sectors

The analysis was also performed on specific central government, local government and health sectors. The analysis found that incidents were likely to relate to human error for these three sectors between 70% and 82%. 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 96% for central government and 98% for both local government and health sectors.

Central Government Sector		
Human Error Likelihood	**Count**	**Percentage**
Likely	20	80
Possibly	4	16
Unlikely	1	4

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

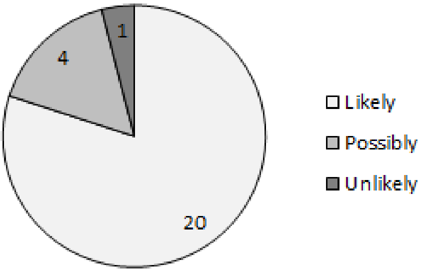

Figure 2 – Likelihood of human error ICO data security incident trends for central government

Local Government Sector		
Human Error Likelihood	**Count**	**Percentage**
Likely	76	81.72
Possibly	15	16.12
Unlikely	2	2.15

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

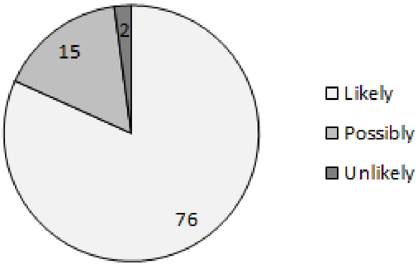

Figure 3 – Likelihood of human error ICO data security incident trends for local government

Health Sector		
Human Error Likelihood	**Count**	**Percentage**
Likely	199	69.09
Possibly	84	29.16
Unlikely	5	1.73

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

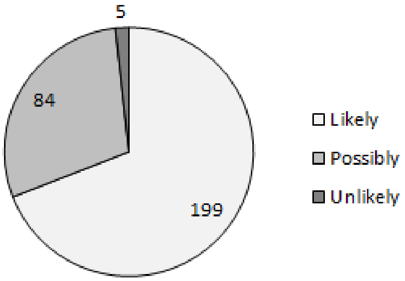

Figure 4 – Likelihood of human error ICO data security incident trends for health

Each of the 148 reported NHS SIRI incidents and associated details were analysed and it was identified that 124 (84%) of the most serious NHS personal data security incidents pertained to human error.

SIRI Level 2 Incidents		
Human Error	**Count**	**Percentage**
Yes	124	83.8
No	24	16.2

Table 7 – NHS SIRI level 2 incidents

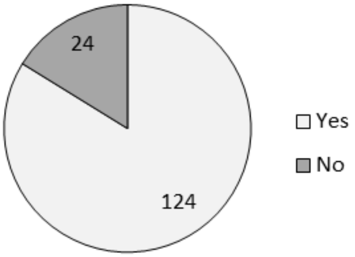

Figure 5 – Proportion of human error for NHS SIRI 2 incidents

This analysis of the Q3 2017 NHS SIRI level 2 incidents found that 42 (34%) were posting an item or information, 31 (25%) were sending an email, and 22 (18%) were safeguarding information or equipment. 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	31	25.00	G
GISAT2 - Entering, updating or deleting data within a system, file or document	5	4.03	D
GISAT3 - Posting an item or information	42	33.87	E
GISAT4 - Configuring a system	1	0.81	C
GISAT5 - Administering a system	0	0.00	D
GISAT6 - Scanning a document	1	0.81	E
GISAT7 - Printing a document	1	0.81	D
GISAT8 - Providing information verbally	2	1.61	D
GISAT9 - Delivering information or equipment	2	1.61	E
GISAT10 - Filing or sorting information	3	2.42	E
GISAT11 - Reading or checking an email, file, document or item	0	0.00	G
GISAT12 - Safeguarding information or equipment	22	17.74	E
GISAT13 – Destroying information or equipment	6	4.84	D
GISAT14 – Accessing a location or environment	0	0.00	D
GISAT15 - Faxing information	2	1.61	D
GISAT16 - Sharing or handing over information or equipment in person	6	4.84	G

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

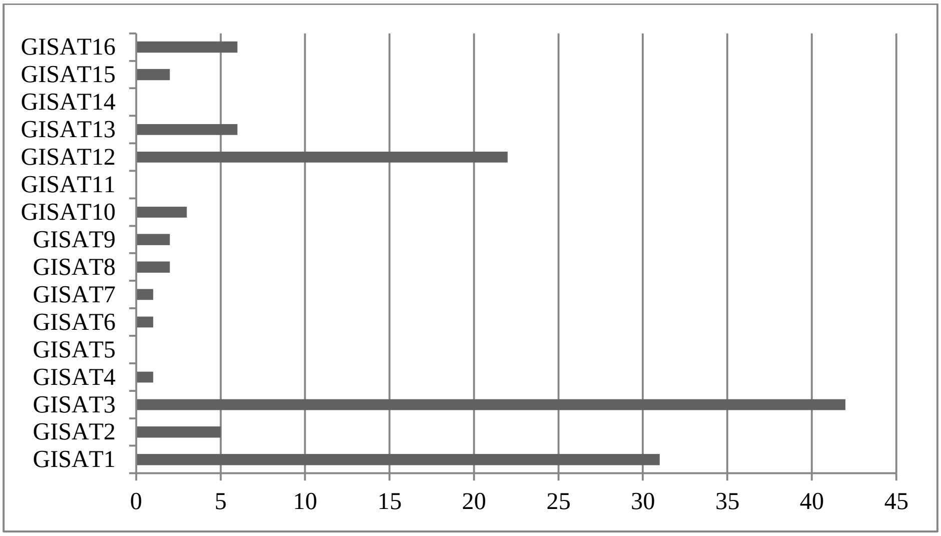

Figure 6 - Mapping of NHS SIRI 2 incidents to GISATs

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 Q3 2017 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, B, F, H or M.

GTT	Count	Percentage
C	1	0.8
D	16	12.9
E	70	56.45
G	37	29.83

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

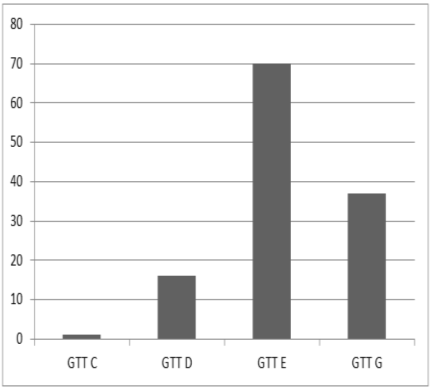

Figure 7 – HEART GTT mapping to NHS SIRI level 2 incidents

5. Discussion

Following analysis of the published data it was identified that 64% of reported incidents across all sectors were likely to be as a result of human error, which aligns to the research published by (Alavi et al., 2016; Stewart and Jürjens, 2017). In addition a further 27% could also possibly be as a result of human error. Therefore, the analysis found that 91% 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 148 reported NHS SIRI level 2 incidents and associated details were analysed and it was identified that 124 (84%) of the most serious NHS personal data security incidents pertained to human error which again aligns to published research (Asai and Hakizabera, 2010).

Following analysis of the published NHS SIRI level 2 incidents it was identified that the most common general information security affecting task was postage of information 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 routine, highly-practiced, rapid task involving relatively low level of skill.

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 applied human reliability analysis techniques applied within the safety field. The application, and adaptation, of methods of working applied 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.

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

7. References

Alavi R, Islam S, Mouratidis H. An information security risk-driven investment model for analysing human factors. Inf Comput Secur 2016;24:205–27. doi:10.1108/ICS-01-2016-0006.

Asai T, Hakizabera AU. Human-related problems of information security in East African cross-cultural environments. Inf Manag Comput Secur 2010;18:328–38. doi:10.1108/09685221011095245.

Chandler T, Chang J, Mosleb A, J. M, Boring R, Gertman D. Human Reliability Analysis

Methods Selection Guidance for NASA. Natl Aeronaut Sp Adm 2006:175.

Department of Health. IG Publications. 2017.

Evans M, Maglaras L, He Y, Janicke H. HEART-IS: A Novel Technique fro Evaluating Human Error-Related Information Security Incidents. Computers & Security, 2018;Submitted.

Evans M, Maglaras LA, He Y, Janicke H. Human behaviour as an aspect of cybersecurity assurance. Secur Commun Networks 2016;9:4667–79. doi:10.1002/sec.1657.

Frangopoulos ED, Eloff MM, Venter LM. Human Aspects of Information Assurance: A Questionnaire-based Quantitative Approach to Assessment 2014.

Furnell S, Khern-am-nuai W, Esmael R, Yang W, Li N. Enhancing security behaviour by supporting the user. Comput Secur 2018;75:1–9. doi:10.1016/j.cose.2018.01.016.

Halevi T, Memon N, Lewis J, Kumaraguru P, Arora S, Dagar N, et al. Cultural and psychological factors in cyber-security. Proc 18th Int Conf Inf Integr Web-Based Appl Serv 2017;13:43–56.

Information Commissioner’s Office. Data security incident trends. 2017.

Komatsu A, Takagi D, Takemura T. Human aspects of information security. Inf Manag Comput Secur 2013;21:5–15. doi:10.1108/09685221311314383.

Lacey D. Understanding and transforming organizational security culture. Inf Manag Comput Secur 2010;18:4–13. doi:10.1108/09685221011035223.

Lyons M, Adams S, Woloshynowych M, Vincent C. Human reliability analysis in healthcare : A review of techniques. Int J Risk Saf Med 2004;16:223–37.

Mahfuth A, Yussof S, Baker AA, Ali N. A systematic literature review: Information security culture. 2017 Int. Conf. Res. Innov. Inf. Syst., IEEE; 2017, p. 1–6. doi:10.1109/ICRIIS.2017.8002442.

Metalidou E, Marinagi C, Trivellas P, Eberhagen N, Skourlas C. The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Soc Behav Sci 2014;147:424–8. doi:10.1016/J.SBSPRO.2014.07.133.

Parsons K, Calic D, Pattinson M, Butavicius M, McCormac A, Zwaans T. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Comput Secur 2017;66:40–51. doi:10.1016/j.cose.2017.01.004.

Stewart H, Jürjens J. Information security management and the human aspect in organizations. Inf Comput Secur 2017;25:494–534. doi:10.1108/ICS-07-2016-0054.

Werlinger R, Hawkey K, Beznosov K. An integrated view of human, organizational, and technological challenges of IT security management. Inf Manag Comput Secur 2009;17:4–19. doi:10.1108/09685220910944722.

Williams JC. A User Manual for the HEART Human Reliability Assessment Method 1992.