IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 10, 2019, accepted June 27, 2019, date of publication July 5, 2019, date of current version August 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2927195

Employee Perspective on Information Security Related Human Error in Healthcare: Proactive Use of IS-CHEC in Questionnaire Form

MARK EVANS[1], YING HE[1], CUNJIN LUO[2,3], IRYNA YEVSEYEVA[1], HELGE JANICKE[1], AND LEANDROS A. MAGLARAS[1]

[1]Cyber Security Centre, De Montfort University, Leicester LE1 9BH, U.K.
[2]Key Laboratory of Medical Electrophysiology, Ministry of Education, Institute of Cardiovascular Research, Southwest Medical University, Luzhou 646000, China
[3]School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China

Corresponding authors: Ying He (ying.he@dmu.ac.uk) and Cunjin Luo (cunjin.luo@yahoo.co.uk)

This work was supported by the National Natural Science Foundation of China (NSFC) under Grant 61803318.

ABSTRACT The objective of the research was to establish data relating to underlying causes of human error which are the most common cause of information security incidents within a private sector healthcare organization. A survey questionnaire was designed to proactively apply the IS-CHEC information security human reliability analysis (HRA) technique. The IS-CHEC technique questionnaire identified the most likely core human error causes that could result in incidents, their likelihood, the most likely tasks that could be affected, suggested remedial and preventative measures, systems or processes that would be likely to be affected by human error and established the levels of risk exposure. The survey was operational from 15th November 2018 to 15th December 2018. It achieved a response rate of 65% which equated to 485 of 749 people targeted by the research. The research found that, in the case of this particular participating organization, the application of the IS-CHEC technique through a questionnaire added beneficial value as an enhancement to a standard approach of holistic risk assessment. The research confirmed that the IS-CHEC in questionnaire form can be successfully applied within a private sector healthcare organization and also that a distributed approach for information security human error assessment can be successfully undertaken in order to add beneficial value. The results of this paper indicate, from the questionnaire responses supplied by employees, that organizational focus on its people and their working environment can improve information security posture and reduce the likelihood of associated information security incidents through a reduction in human error.

INDEX TERMS Human error assessment and reduction technique (HEART), human error related information security incidents, human reliability analysis (HRA), information security, IS-CHEC.

I. INTRODUCTION

It is acknowledged that people play a crucial role in the security of information [1], which is the lifeblood of a company [2], and this is not just an IT problem [2]–[4]. Yet there continues to be varied understanding of the proportions of human error resulting in regular information security incidents and breaches [5], [6] and the level of risk exposure [7] which cannot be ignored [8] within the information security community encompassing both academia and industry.

Furnell *et al.* [9] published results indicating rates of human error related to incidents was as low as 7.9% but an earlier dataset relating to 2005 suggested that human error was the largest category at 42%. Contrary to these figures, Lacey [10] stated that the majority of security incidents are caused by human factors and his research also presented that almost 90% of workplace accidents are caused by human failure. In addition, Hals [11] stated that human error is the primary causal factor in 70%-80% of accidents in the oil and gas industry suggesting that the information security community could learn from the safety field which is more established in this area [12]–[15].

Other research presented that 24% of data loss incidents were caused by insiders including accidental and malicious acts [16], 55% of root causes of data breaches occurred as a result of unintentional employee action [17] and more than

The associate editor coordinating the review of this manuscript and approving it for publication was Zheng Yan.

 This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

one-third of hospital communication errors were related to human factors. In addition, it is also published that most unintended and unanticipated errors are due to socio-technical issues when using technologies [18] which are leading to the socio-technical nature of information security coming to the fore [19]. The Annual Information Governance Incident Trends (2015-2016) [20] presented that 77% of incidents were made up of disclosure in error, lost or stolen paperwork and unauthorized access/disclosure.

The majority of reported information security incidents and breaches within organizations are as a result of human error [21], [22]. This was confirmed based upon an analysis of published incidents and breaches [23], [24]. Nonetheless, there is a lack of empirical information security research [19] regarding organizational theories. This lack of focus include limited attention on the topic of human error and the effects it has on information security assurance and associated incidents and breaches as shown by the UK Government Cyber Security Breaches Survey 2019 [25]. Despite there now being a common understanding that human error should be a primary focus within organizations, due to the risks that people pose [26], the survey [25] does not encompass this common non-technical concern unlike in previous surveys [27].

This case study forms part of wider research where in our previous empirical research with public and private sector healthcare organizations we presented that human reliability analysis (HRA) is applicable and beneficial [21], [22], [28] to an information security context. However, the developed and empirically validated [21], [22] Information Security Core Human Error Causes (IS-CHEC) information security HRA technique had so far only been used reactively in relation to reported information security incidents in healthcare. As stated by Gu *et al* [29] human reliability should be extended to address the entire information security risk management function. There is currently no published information security HRA technique or method that is designed to proactively interact directly with employees in order to identify potential causes of human error which may result in an information security incident and the associated risk exposure.

The approach taken in this article was to adapt the IS-CHEC technique [22] into survey questionnaire form and deploy it to enable the participating organization to act upon the results whilst enhancing academic knowledge in this area. This included expanding upon the IS-CHEC analysis element [21] to enable quantification of risk based upon the participating organization's risk quantification mechanisms. In addition, the IS-CHEC mapping element [21] was adapted to become a questionnaire data capture element capturing underlying human error cause data, the business area the employee works in and business processes involved in to obtain valuable contextual data.

We distributed the IS-CHEC questionnaire to all operational personnel within a participating private sector healthcare organization to obtain their views and opinions about the causes of human error, the tasks that would be most likely affected by human error and suggested preventative measures that would address the human error problem and resultant information security incidents.

The results of the survey were then broken down into the 9 distinct operational business areas of the participating organization to allow a more granular understanding in terms of the perceived underlying causes of human error, the business processes most likely affected and the specific supporting tasks, such as updating systems or sending emails, that would be most susceptible to human error. Moreover, through mutual analysis of the survey questionnaire results with the respective Director or Head of each of the operational business areas the level of risk exposure was established based upon the classification of data being processed by each task and process, the established human error probability and automatically mapping these to the participating organizations risk quantification metrics.

We also compared the results with each area's incident trends and also a separate information security risk assessment that had been carried out within the previous 12 months for each operational business area. The comparison was intended to identify the beneficial value of the questionnaire to the participating organization as an enhancement to standard risk assessment undertaken by a dedicated information security employee.

The survey was operational from 15th November 2018 to 15th December 2018 and used Microsoft Office 365 Forms technology. It achieved a response rate of 65% which equated to 485 of 749 people targeted by the research.

The motivation behind this case study was to obtain detailed data in relation to the causes of human error which has been proven to be the most common root cause of information security incidents within the participating healthcare organization. The survey questionnaire was designed to proactively apply the IS-CHEC human reliability analysis technique that has proved to be successful when applied to incident management [21], [22]. The IS-CHEC technique questionnaire aimed to identify the following:

- The most likely Core Human Error Causes (CHEC) that could result in incidents and their likelihood.
- The most likely tasks (referred to as GISATs by the IS-CHEC technique) that could be affected by human error.
- The suggested most important remedial and preventative measures (RPM) to address the human error concern.
- Ascertain the systems or processes that would likely be affected by human error.
- Establish the levels of risk exposure based upon the likelihood responses obtained and the impact of human error based on analysis with the participating organization Directors and Heads of Service. Risk values also leverage the upper and lower bounds of tolerance of human error probability as set out within the Human Error Assessment and Reduction Technique (HEART) HRA technique.

This paper makes the following contributions:

- Conducts for the first time in literature dedicated empirical case study research within a participating healthcare organization to establish employee perceptions of information security weaknesses related directly to human error
- Converts, applies and evaluates the IS-CHEC technique in survey questionnaire form designed to proactively capture the causes of human error, the tasks that would be most likely affected and suggested remedial and preventative measures
- Assessment of whether the calibrated IS-CHEC technique could be applied within a participating private sector healthcare organization via distributed questionnaire and add beneficial value when compared to standard security assessments performed by a security professional

The remainder of this paper is structured as follows. Section 2 details the associated related work including related information security work and associated literature. Section 3 presents the research method including the case study participating organization, the IS-CHEC questionnaire design and analysis approach. Section 4 presents the results of the questionnaire survey and comparison with independent information security risk assessment. Section 5 presents the findings, implications, comparisons with the literature and any limitations of the method and technique. Finally, section 6 captures the research conclusions.

II. RELATED WORK

Taniuchi *et al.* [30] presented that human error is a deviation from required performance whereas Hals [11] presented a view that human error pertains to human actions that exceed a limit of acceptability. Furnell *et al.* [31] presented in their work that poor computer and information security is caused by non-deliberate accidental human actions. Reason [32] classified human errors in three categories. These classifications are defined [11] as a slip which is a correct action but a faulty execution, a lapse which is a lapse in memory or distraction causing a failed execution of a task, and a mistake which is defined as a correct execution of an incorrect intention.

Hadlington *et al* [33] as part of their research into work identity and work locus of control and its relationship with information security awareness state that there has currently been limited success in mitigating the threat posed by accidental attempts to gain access to company data and systems. They also present that there is now a greater focus in the human aspects of information security and that technology cannot be the only solution. Notably, they highlight that a greater understanding of why employees fail to adhere to the most basic information security principles is critically important to enable comprehensive frameworks to be developed. In addition, they investigate the degree of work locus of control and conclude that employees having limited perceived control over their workplace environments were more likely to have weaker information security awareness.

Compliance intention is defined as the intention of the employee to protect the information resources of the organization from potential security breaches [34] and they tend to be disinterested if the benefit of information security compliance is not sufficient when compared to the cost. Veiga and Martins [35] argue that one of the most effective countermeasures against human factor threats to information security are awareness, training and education and that although there might be adequate technology and processes in place, employees might circumvent controls because of their perception or attitude towards information security policy. Cilliers [36] states the most common data breach still remains where employees that have access to or may copy information without authorization. There are also a number of theories that have been published [16], [37] including deterrence theory (DT), theory of reasoned action/planned behavior (TRA), protection motivation theory (PMT), rational choice theory (RCT), social cognitive theory (SCT), social bond theory (SBT), and neutralization theory (NT), which address modeling behavior or behavioral change. However, all of these theories appear to focus upon intentional action and not address the prominent issue of unintentional human error.

Hals [11] presented three human error causation paradigms which were the engineering error paradigm, individual error paradigm and organizational paradigm in their work. These paradigms look to identify the underlying causes of human error, which could be contributing factors of system failures [38] and are known as different terms including Core Human Error Cause (CHEC) [21], Error Producing Condition (EPC) [39] or Performance Shaping Factors (PSF) [40]. These terms form part of human reliability analysis (HRA) techniques and their goal is to assess the risks attributable to human error for ways of reducing system vulnerability [11]. In order to achieve this HRA goal, the technique must achieve human error identification, human error quantification and human error reduction [11]. An example of an HRA technique is the Human Error Assessment and Reduction Technique (HEART), which is based on the general principle that for each task in life there is a basic probability of failure [41]. The underlying causes of error could include humans being over or under-loaded as well as considering physical and mental task demands [42], [43] or social factors [44], which could indicate whether the environment makes it possible to exhibit or impact upon secure behavior [45], [46].

As stated by Colwill [26], security assessments must take into account explicitly human behavior. Questionnaires with a focus on the human factors have been established, validated and published previously. These include the Human Aspects of Information Security Questionnaire (HAIS-Q) [47], [48] and the Cyber Human Error Assessment Tool [49]. The HAIS-Q [47] employs a questionnaire comprising of 63 statements spanning 7 focus areas (Internet use, email use, social networking site use, password management, incident reporting, information handling and mobile computing) in order to

measure employee information security knowledge, attitude and behavior. The HAIS-Q questionnaire is broader than solely focusing upon human error as it also incorporates intentional conscious and/or malicious employee behavior as well as the possibility for employees to be exploited by malicious third parties. The CHEAT questionnaire [50] is specifically focused upon cyber security human error using techniques such as HEART and was developed based upon previously published incident data. However, it was constrained by the lack of information in the public domain [50]. It comprises of 41 human factor indicators spanning into four categories (people, organization, environment and technology).

III. MATERIALS AND METHOD

A. PARTICIPATING PRIVATE SECTOR ORGANISATIO

The case study benefitted from a participating private sector organization that provides healthcare services to the British National Health Service (NHS). They are a large service provider operating in the United Kingdom. It has approximately 1100 employees and provides a range of services. Its incident management practices are required to support compliance with international security standards such as the ISO27001 Standard, Cyber Essentials as well as the NHS Information Governance Toolkit [51]. Information security is governed centrally by the Senior Information Risk Owner and associated team who are responsible for the development of organizational strategy and policy. In addition, designated information security leads have responsibility for every business area to ensure full coverage and adherence.

B. IS-CHEC QUESTIONNAIRE DESIGN

The targeted survey questionnaire participants encompassed all of the 749 operational employees of the participating organization. This incorporated all operational roles from the Head of each business area through to all operatives and there were no exclusions. Respondent participation was anonymous and therefore unable to be enforced for all personnel but was strongly encouraged and response rates monitored by management throughout the duration of the survey. To conduct research involving human participants, this research adhered to De Montfort University (DMU) ethical standards and guidelines, and has been approved by the DMU ethics committee (ref: 1516/325). Operational areas of the participating organization were selected due to previous empirical research [21] identifying that virtually all information security incidents related to operational areas of the business. In addition, the operational areas of the business had been subject to information security risk and compliance assessments over the previous 12 months which would enable comparison to be undertaken. The non-operational areas of the business had low numbers of incidents which did not provide a reliable data set for comparison and also had not been subject to information security risk and compliance assessment which prevented comparison.

The electronic questionnaire was designed to take no longer than 5 minutes to complete and focuses on capturing quality information easily from the user using the Microsoft Office 365 Forms technology. It was intended to proactively use the IS-CHEC technique through distributed questionnaire and compare the results to an information security risk assessment undertaken by information security personnel independent of this research. The questionnaire obtained the likelihood element of the risk assessment approach. The impact will be applied by the Director or Head of each respective business area and researcher through an understanding of the information assets associated with the business area and organization's systems or processes identified by employees as being vulnerable to human error. In order to encourage higher response rates a prize was offered for the participating organization operational business area with the greatest response rate percentage.

The questionnaire comprises of 16 questions which are presented in Table 7 in the appendices of this paper. These questions are comprised of 10 drop-down list questions, 3 Likert scale questions, and 3 short answer text boxes. Six of the questions are mandatory and 10 are optional. The mandatory questions are made up of 4 drop-down list questions, 1 Likert scale question, and 1 short answer text box. The optional questions are made up of 6 drop-down list questions, 2 Likert scale questions, and 2 short answer text boxes. However, the questionnaire was designed to enable relevant questions to be skipped if a 'not applicable' response was provided for associated preceding questions. In addition, the questionnaire drop-down list response options were automatically randomized to remove any bias in selection.

The questionnaire had an introductory section prior to the 16 questions (See Appendix A1), briefing the participants that their involvement is voluntary, the study will be conducted in an anonymous way and the benefits of participation.

In order to ensure the questionnaire was fit for purpose prior to deployment a targeted multi-disciplinary pilot group of 12 people was agreed to test and review the created IS-CHEC questionnaire. Changes to the questionnaire were agreed by the Information Security Steering Group and applied based upon their feedback. The pilot group comprised of the participating organization Information Security Team, Chief Operating Officer, Senior Information Risk Owner, Communications Team, Head of Risk Management and Compliance, Head of Clinical Governance and an independent proof reader. Due to the large number of CHECs available within the IS-CHEC technique it was felt by the participating organization that this could be confusing and difficult for the respondents which could affect the overall response rate. Therefore a decision was taken to only use the CHECs that had been previously identified by the participating healthcare organization and also those identified by the public sector healthcare organization as part of the wider empirical study [21], [22]. These CHECs can be seen in Table 2. In addition, the wording of the CHECs were reviewed and simplified to aid understanding of the questionnaire respondents

which would enable faster completion and greater accuracy of responses.

In order to conduct the empirical study, the IS-CHEC technique and tool was used as presented in our previous study within a private sector organization [21]. The IS-CHEC technique is an adapted version of the HEART HRA technique [39].

C. ANALYSIS METHOD

The analysis and computation of the findings were undertaken using an adaptation of the IS-CHEC mapping and analysis elements as published within previous articles [21], [22]. This enabled questionnaire data capture, repeatable practices, easy computation and reporting in accordance with the participating organization's risk appetite, risk framework and associated risk matrix based upon understanding of the probability and impact of a risk event occurring. This was achieved through establishing the classification of the data processed by each organization system or process and supporting tasks captured within the questionnaire responses. The classification could then be mapped to the organization's risk appetite standard and associated risk impact classifications. The HEART calculations were applied as part of the IS-CHEC analysis element to establish a nominal human error probability which could also be mapped to the organization's risk appetite standard and associated risk probability classifications. The capturing of both the risk impact and probability using the organization's own risk quantification mechanisms enabled accurate, understandable and automatic risk exposure quantification. The IS-CHEC questionnaire data capture and questionnaire analysis elements are presented in Tables 7 and 8 respectively which can be found within the appendices of this paper.

In order to establish if the IS-CHEC questionnaire could add beneficial value, the results were split into each of the 9 operational business areas within the participating organization targeted by the questionnaire and subsequently compared to actual incidents experienced for each area. This paper presents the consolidated results for each area however a comprehensive and detailed report was compiled for the participating organization at the conclusion of the survey to enable targeted action to be planned and undertaken. A detailed analysis was performed looking at incident root causes as well as the underpinning core human error causes where the incident had been determined to be as a result of human error by looking at core components of the IS-CHEC technique (CHEC, GISAT, RPM and System or Process). Results were subsequently compared to information security risk and compliance assessment reports undertaken independently of this research for each area. This comparison was undertaken to understand how close the IS-CHEC questionnaire results were to actual incident exposure in terms of identifying underlying vulnerabilities or weaknesses compared to a standard information security risk and compliance assessment undertaken by a large organization as part of ISO27001 [52] compliance activity.

TABLE 1. Business area response rates.

Business Area	Count of Questionnaire Completions	Count of Staff	Percentage
A	35	69	51%
B	47	55	85%
C	64	109	59%
D	13	20	65%
E	66	84	79%
F	124	230	54%
G	49	62	79%
H	72	104	69%
I	15	16	94%
Total	**485**	**749**	**65%**

IV. RESULT

As outlined earlier in the paper the questionnaire was active from 15th November 2018 to 15th December 2018. It achieved a response rate of 65% as presented in Table 1. This equated to 485 of 749 people targeted by the research. The average time taken to complete the questionnaire was 13 minutes 30 seconds. The results were broken down by the 9 operational business areas of the participating organization. The name of each business area has been redacted and

TABLE 2. Total CHECs.

CHEC	Most Likely CHEC Count	2nd Most Likely CHEC Count	3rd Most Likely CHEC Count	Total Count
CHEC36 - Pressure to work too fast	136	57	30	223
CHEC2 - A shortage of time	31	42	50	123
CHEC16 - Inaccurate or incomplete information	37	49	36	122
CHEC29 - Stress	34	38	40	112
CHEC15 - Operator inexperience	23	46	39	108
CHEC17 - Little or no checking or testing by another person	15	31	29	75
CHEC11 - Don't understand the policy, standards, process or procedures	26	21	26	73
CHEC9 - Learning a new technique, process, procedure or way of working	17	29	26	72
CHEC13 - System information communicated is inaccurate, unclear or inappropriate	26	23	15	64
CHEC34 - Inactivity or highly repetitious tasks	18	22	22	62
CHEC19 - Not enough information	21	15	19	55
CHEC6 - A misunderstanding between an operator and a designer of a procedure	19	11	15	45
CHEC28 - Unaware of the importance of your tasks to the wider service	14	9	12	35
CHEC39 - No self-checking or testing	12	12	7	31
CHEC7 - No way to undo an error	6	12	10	28

TABLE 3. Total GISATs.

GISAT	Most Likely GISAT	2nd Most Likely GISAT	3rd Most Likely GISAT	Total Count
GISAT2 - Entering, updating or deleting data within a system, file or document	224	72	35	331
GISAT1- Sending an email	49	59	40	148
GISAT5 - Administering a system	47	49	35	131
GISAT11 - Reading or checking an email, file, document or item	31	41	45	117
GISAT10 - Filing or sorting information	21	39	23	83
GISAT8 - Providing information verbally	30	18	20	68
GISAT3 - Posting an item or information	14	20	22	56
GISAT16 - Sharing or handing over information or equipment in person	16	17	19	52
GISAT9 - Delivering information or equipment	20	13	17	50
GISAT12 - Safeguarding information or equipment	11	18	14	43
GISAT4 - Configuring a system	6	16	9	31
GISAT14 – Accessing a location or environment	5	3	9	17
GISAT13 – Destroying information or equipment	4	7	4	15
GISAT6 - Scanning a document	3	5	5	13
CHEC	**Most Likely CHEC Count**	**2nd Most Likely CHEC Count**	**3rd Most Likely CHEC Count**	**Total Count**
CHEC1 - Unfamiliarity due to infrequent or new situation	14	3	10	27
CHEC23 - Unreliable instrumentation or equipment	12	8	6	26
CHEC8 - Monitoring numerous computer monitors or items	12	6	4	22
CHEC12 - Don't understand risk	4	6	9	19
CHEC26 - No way to keep track of progress	4	6	5	15
CHEC4 - Too easy to switch off, disable or incorrectly modify alerts, notifications or messages	2	4	5	11
CHEC3 - Too many alerts, notifications, messages	2	1	4	7

GISAT	Most Likely GISAT	2nd Most Likely GISAT	3rd Most Likely GISAT	Total Count
GISAT7 - Printing a document	3	4	2	9
GISAT15 – Faxing information	1	2	3	6

TABLE 4. Total RPMs.

Suggested Preventative Measure	Most Suggested Preventative Measure	2nd Most Suggested Preventative Measure	3rd Most Suggested Preventative Measure	Total Count
RPM1 – Awareness and training undertaken (including 1:1)	87	87	64	238
RPM2 – Procedures documented and communicated	35	49	31	115
RPM4 – Recruitment of additional staff	47	23	31	101
RPM5 – Change to, simplification or standardisation of existing procedures, tools, systems or practices	59	38	0	97
RPM6 – Increased supervision or checks	41	30	21	92
RPM12 – Incentives introduced	29	25	24	78
RPM13 – Acquire and introduce new tools or technology	25	23	16	64
RPM7 – Change to communication methods	24	22	18	64
RPM16 – Eliminate or reduce distractions	19	20	17	56
RPM10 – Change to work patterns such as frequent breaks	21	20	14	55
RPM8 – Risk assessment or audit undertaken and acted upon	23	13	11	47
RPM18 – Introduce warnings, alerts or alarms	13	10	16	39
RPM11 – Job rotation	19	11	9	39
RPM15 – Split process and introduce segregation of duties	8	11	10	29
RPM3 – Simulation exercises performed	4	11	9	24
RPM14 – Introduce robotics/automation/artificial intelligence	14	5	3	22
RPM9 – Job description checked and updated	7	3	7	17
RPM20 – Reissue or resend information or equipment	5	7	3	15
RPM17 – Eliminate look-and-sound-alikes	2	4	2	8
RPM19 – Recover, collect or destroy information or equipment	3	3	2	8
RPM0 – None needed	0	0	0	0
RPM99 – Other non-human error related remedial and preventative measure	0	0	0	0

TABLE 5. Participating organization root cause categories.

Root Cause Categories
RC1 – Human Error Slip or Lapse (Unintentional)
RC2 – Human Factor (Intentional Act. E.g. hacking or non-compliance with policy)
RC3 – Technology Failure or Configuration
RC4 – Procedural Mistake or failure
RC5 - Physical Control Failure

replaced with a letter in order to protect the identity of the participating organization. Each business area forms different aspects of healthcare administration specific to their business purpose.

The IS-CHEC questionnaire and the method outlined earlier identified that there were 26 of the responses that were quantified as having the highest possible risk score

TABLE 6. Comparison of questionnaire results against previously captured incident and risk assessment data.

Business Area	Correlation with Incident Data				Comparison with Risk and Compliance Assessment	
	Total CHEC	Total GISAT	Total RPM	% Human Error	Action Root Cause Focus	IS-CHEC Questionnaire Added Value?
A	Yes	Yes	Yes	76%	• RC1 – 0 • RC2 – 5 • RC3 – 2 • RC4 – 6 • RC5 – 4	Yes
B	Yes	Yes	Yes	100%	• RC1 – 1 • RC2 – 1 • RC3 – 0 • RC4 – 4 • RC5 - 2	Yes
C	Yes	Yes	Yes	78%	• RC1 – 1 • RC2 – 5 • RC3 – 1 • RC4 – 2 • RC5 - 4	Yes
D	No	Yes	No	100%	• RC1 – 0 • RC2 – 2 • RC3 – 3 • RC4 – 1 • RC5 - 2	Yes
E	Yes	Yes	Yes	94%	• RC1 – 0 • RC2 – 3 • RC3 – 2 • RC4 – 1 • RC5 - 7	Yes
F	Yes	Yes	Yes	91%	• RC1 – 1 • RC2 – 3 • RC3 – 2 • RC4 – 7 • RC5 - 8	Yes
G	Yes	Yes	Yes	88%	• RC1 – 0 • RC2 – 3 • RC3 – 1 • RC4 – 1 • RC5 - 2	Yes
H	No	Yes	Yes	92%	• RC1 – 0 • RC2 – 4 • RC3 – 3 • RC4 – 5 • RC5 - 8	Yes
I	No	Yes	Yes	97%	• RC1 – 0 • RC2 – 2 • RC3 – 2 • RC4 – 2 • RC5 - 2	Yes

of 16 based on the 4 (probability) x 4 (impact) risk matrix used by the participating organization. These identified risks spanned across 6 of the 9 business areas. The participating organization expressed that the results were useful as the respondents made it clear that there were particular organizational systems or processes that cause them the greatest concern in terms of its associated data and the effect of potential human error.

The IS-CHEC technique questionnaire captures between 1-3 CHECs, GISATs and suggested RPMs. Therefore the following text shows the captured results for the CHEC, GISAT and RPM components and then combines to provide a total count for each component. Any questionnaire response that had duplicate CHEC, GISAT or suggested preventative measure selected had the duplicates removed to ensure the accuracy of overall results for each IS-CHEC component.

TABLE 7. IS-CHEC questionnaire data capture element.

No.	Question	Description
1	Which business area do you work in?	This is a mandatory question using a drop-down list to select the business area the user works in.
2	Most likely cause of human error? Please select the most likely potential causes of errors that could lead to information governance and security incidents whilst you are performing your work.	This is a mandatory question using a drop-down list with randomly shuffled options to remove bias. Only the Core Human Error Causes (CHEC) that have been selected by participating organisations within our previous wider empirical research [21], [22] have been included in the options in order to reduce the options from 40 to 22. It was perceived during review with the private sector organisation that 40 options would be too much for the users and therefore this suggestion was made to the researcher. Also the text for each of the 22 CHECs was simplified as the private sector organisation felt that standard users would not fully understand the CHECs in there full format.
3	How likely is this cause?	This is a mandatory question. A simplified Likert scale is provided with 5 options with wording for each to make it easier for population. The 5 options is less granular that the IS-CHEC incident analysis method (11 options) but it is felt that this would be sufficiently granular and the Microsoft Forms software only allowed a maximum of 7 options. The options are listed below. This could be adjusted for each organisation using their own risk quantification policy. 0 - Not possible 0.2 – Unlikely 0.5 – Possible 0.8 Highly likely 1.0 Definitely will happen
4	Second most likely cause of human error? (Optional) Please select the second most likely potential causes of errors that could lead to information governance and security incidents whilst you are performing your work. If there is not a second most likely cause of human error please select 'Not Applicable'.	This is an optional question using a drop-down list which does not use randomly shuffled answers in order for the 'Not Applicable' option to be at the top for the ease of the user. The same criteria have been applied as in question 2. If an option of 'Not Applicable' is selected then the questionnaire automatically skips to question 8.
5	How likely is this cause?	This is an optional question. The same criteria has been applied as in question 2.
6	Third most likely cause of human error? (Optional) Please select the third most likely potential causes of errors that could lead to information governance and security incidents whilst you are performing your work. If there is not a third most likely cause of human error please select 'Not Applicable'.	This is an optional question using a drop-down list which does not use randomly shuffled answers in order for the 'Not Applicable' option to be at the top for the ease of the user. The same criteria have been applied as question 2. If an option of 'Not Applicable' is selected then the questionnaire automatically skips to question 8.
7	How likely is this cause?	This is an optional question. The same criteria has been applied as in question 2.
8	Most likely task affected? Please select the task that is most likely to be affected by the core human error causes you selected above.	This is a mandatory question using a drop-down list with randomly shuffled options to remove bias. All 16 IS-CHEC General Information Security Affecting Tasks (GISAT) are presented to the user.
9	Second most likely task affected? (Optional) Please select the task that is second most likely to be affected by the core human error causes you selected above. If there is not a second most likely task affected please select 'Not Applicable'.	This is an optional question using a drop-down list which does not use randomly shuffled answers in order for the 'Not Applicable' option to be at the top for the ease of the user. The same criteria have been applied as in question 8. If an option of 'Not Applicable' is selected then the questionnaire automatically skips to question 11.
10	Third most likely task affected? (Optional) Please select the task that is third most likely to be affected by the core human error causes you selected above. If there is not a third most likely task affected please select 'Not Applicable'.	This is an optional question using a drop-down list which does not use randomly shuffled answers in order for the 'Not Applicable' option to be at the top for the ease of the user. The same criteria have been applied as question 8. If an option of 'Not Applicable' is selected then the questionnaire automatically skips to question 11.
11	Most important suggested preventative measure? Please select a suggested preventative measure that you feel is most likely to help you and your colleagues to perform your work successfully and avoid errors that lead to information security incidents.	This is a mandatory question using a drop-down list with randomly shuffled options to remove bias. All 20 IS-CHEC Remedial and Preventative Measures (RPM) are presented to the user.
12	Second most important suggested preventative measure? (Optional) Please select a suggested preventative measure that you feel is second most likely to help you and your colleagues to perform your work successfully and avoid errors that lead to information security incidents. If there is not a second most important suggested preventative measure please select 'Not Applicable'.	This is an optional question using a drop-down list which does not use randomly shuffled answers in order for the 'Not Applicable' option to be at the top for the ease of the user. The same criteria have been applied as in question 11. If an option of 'Not Applicable' is selected then the questionnaire automatically skips to question 14.

TABLE 7. *(Continued.)* **IS-CHEC questionnaire data capture element.**

13	Third most important suggested preventative measure? (Optional) Please select a suggested preventative measure that you feel is third most likely to help you and your colleagues to perform your work successfully and avoid errors that lead to information security incidents. If there is not a third most important suggested preventative measure please select 'Not Applicable'.	This is an optional question using a drop-down list which does not use randomly shuffled answers in order for the 'Not Applicable' option to be at the top for the ease of the user. The same criteria have been applied as question 11. If an option of 'Not Applicable' is selected then the questionnaire automatically skips to question 14.
14	Most likely affected system or process? Please enter the system, process or activity that you feel would most likely be affected by human error and lead to an information governance and security incident from your area of work. Do not enter confidential personal data into the text box below.	This is a mandatory short answer text box. The use of a short answer text box was due to both participating organisations not having a list of systems and processes or a list which would be understandable to all users. Also a short answer text box reduces the opportunity for confidential information to be added to the response form. In addition, the note below is added to the question sub-title: *Do not enter confidential personal data into the text box below.*
15	Second most likely affected system or process (Optional) Please enter the system, process or activity that you feel would second most likely be affected by human error and lead to an information governance and security incident from your area of work. Do not enter confidential personal data into the text box below.	This is an optional short answer text box. The same criteria have been applied as question 14.
16	Third most likely affected system or process (Optional) Please enter the system, process or activity that you feel would third most likely be affected by human error and lead to an information governance and security incident from your area of work. Do not enter confidential personal data into the text box below.	This is an optional short answer text box. The same criteria have been applied as in question 14.

Generically across the participating organization, the responses showed clearly that the respondents felt they were being made to perform their work at a faster rate than they are comfortable with. 136 of the 485 respondents felt that this was the most likely cause of human error which equates to 28%. However, also taking into account the second and third most likely CHEC then this accounted for 223 responses or 46%. The total responses related to the CHECs are presented in Table 2 and a break-down by business area is shown in Table 9.

In terms of the most likely GISAT that would be affected by human error again the results were very clear with 224 of the 485 (46%) respondents stating that the most likely task that would be affected by human error would be entering, updating or deleting data within a system, file or document. Taking into account the most, second and third likely task to be affected then this was also the same GISAT and accounted for 331 (68%) responses. Interestingly the second most common GISAT for the most, second and third most likely and also the total of all responses was sending an email which accounted for 148 (31%) of all responses. The total responses related to the GISATs are presented in Table 3 and a break-down by business area is shown in Table 10.

The respondents were also asked to suggest the RPMs that should be applied in order to reduce or avoid the current volumes of human error. Again the results were very clear in that the employees were suggesting greater focus to be placed on awareness and training. This was the most common response for the most, second and third most important suggested preventative measure and accounted for 238 (49%) of all responses. The total responses related to the suggested preventative measures are presented in Table 4 and a break-down by business area is shown in Table 11.

For each of the 9 organizational business areas within the participating organization the questionnaire results were compared against IS-CHEC incident data and information security risk assessment reports captured since 01/03/2018.

The participant organization incident data utilizes the same IS-CHEC components (CHEC, GISAT, RPM) which enabled correlation with the questionnaire data. The information security assessments, which were independent of this research, focused on all aspects of information security and not solely human error the mapping of root cause analysis of findings was used. The participating organization captured root causes as set out in Table 5.

As presented in Table 6 a comparison of the questionnaire results were compared with past incident data and dedicated information security risk and compliance assessments that were undertaken for each of the 9 organizational business areas independent of this research. The analysis looked at the IS-CHEC questionnaire results and the recorded IS-CHEC components for past information security incidents to see if there was a correlation related to those that were most commonly captured. The analysis of risk and compliance information security assessment reports looked at the selection of human error-related preventative measures for business areas and considered the percentage of human error-related information security incidents recorded

TABLE 8. IS-CHEC questionnaire analysis element.

Field	Description
Actual system or process?	As the system or process field was a free text field it may have been misunderstood and the response may not have been an actual system or process. Therefore this field was added to enable this misinterpretations to be identified
Nominal unreliability	In-built HEART nominal unreliability associated with each GTT. There is no adaptation to this field.[1]
Nominal unreliability lower bound	In-built HEART nominal unreliability lowest value within the techniques range associated with each GTT.[1]
Nominal unreliability upper bound	In-built HEART nominal unreliability highest value within the techniques range associated with each GTT.[1]
Most significant CHEC WoS decimal	A field to remove the textual descriptor applied to options within the questionnaire Likert scale. The output is the numerical response.
Most significant CHEC strength	In-built HEART value/strength assigned to each EPC.[1]
Second most significant CHEC WoS decimal	A field to remove the textual descriptor applied to options within the questionnaire Likert scale. The output is the numerical response.
Second most significant CHEC strength	In-built HEART value/strength assigned to each EPC.[1]
Third most significant CHEC WoS decimal	A field to remove the textual descriptor applied to options within the questionnaire Likert scale. The output is the numerical response.
Third most significant CHEC strength	In-built HEART value/strength assigned to each EPC.[1]
Primary CHEC assessed affect	In-built HEART calculation establishing the effect of each identified HEART EPC which is referred to as a CHEC within the IS-CHEC technique.[1]
Secondary CHEC assessed affect	In-built HEART calculation establishing the effect of each identified HEART EPC which is referred to as a CHEC within the IS-CHEC technique.[1]
Tertiary CHEC assessed affect	In-built HEART calculation establishing the effect of each identified HEART EPC which is referred to as a CHEC within the IS-CHEC technique.[1]
Nominal likelihood of failure	Nominal probability that is employed to characterise the general likelihood of task failure based on the in-built HEART calculation.[1]
Nominal likelihood of failure lower bound	Nominal lowest value probability based on the HEART ranges that are employed to characterise the general likelihood of task failure based on the in-built HEART calculation.[1]
Nominal likelihood of failure upper bound	Nominal highest value probability based on the HEART ranges that are employed to characterise the general likelihood of task failure based on the in-built HEART calculation.[1]
Risk likelihood/probability	Mapping of the Nominal likelihood of failure to the participating organisations quantified risk probability set within their risk appetite standard.
Risk likelihood/probability lower bound	Mapping of the Nominal likelihood of failure lower bound to the participating organisations quantified risk probability set within their risk appetite standard.
Risk likelihood/probability upper bound	Mapping of the Nominal likelihood of failure upper bound to the participating organisations quantified risk probability set within their risk appetite standard.
Data classification	Mapping to the participating organisations data classification standard to enable the risk impact to be established.
Risk impact	Mapping of the data classification to the participating organisations quantified risk impact set within their risk appetite standard.
Risk score	Establishing the numerical risk exposure as per the participating organisations quantified 4x4 risk scoring matrix set within their risk appetite standard.
Level of risk exposure	Mapping of the established numerical risk score to the qualitative terms used by the participating organisation as set within their risk appetite standard.
Risk score lower bound	Establishing the numerical risk lower bound exposure as per the participating organisations quantified 4x4 risk scoring matrix set within their risk appetite standard.
Level of risk exposure lower bound	Mapping of the established numerical risk lower bound score to the qualitative terms used by the participating organisation as set within their risk appetite standard.
Risk score upper bound	Establishing the numerical risk upper bound exposure as per the participating organisations quantified 4x4 risk scoring matrix set within their risk appetite standard.
Level of risk exposure upper bound	Mapping of the established numerical risk upper bound score to the qualitative terms used by the participating organisation as set within their risk appetite standard.

[1] There is no adaptation to this field.

since 01/03/2018. This comparison was undertaken with the participating organization's Information Security Manager and Information Security Incident Analyst. It was concluded by the Information Security Manager that in all 9 organizational business areas the IS-CHEC questionnaire added value and addressed human error gaps within the risk and compliance assessment reports and approach. This was due to the business context whereby the most common root cause of information security incidents is unintentional human error and had not been explicitly catered for within the information security risk and compliance assessments.

V. DISCUSSION

The research has found that in the case of this particular case study and associated participating organization, where it had already been established that human error accounted for the vast majority of reported information security incidents, that the use of the IS-CHEC technique proactively through a questionnaire added beneficial value as an enhancement to the standard approach of holistic risk assessment performed as part of compliance initiatives in conjunction with standards such as ISO27001 [52].

TABLE 9. CHECs by business area.

CHEC	Business Area								
	A	B	C	D	E	F	G	H	I
1	1	4	7	1	2	3	5	4	0
2	16	7	23	1	9	36	11	18	2
3	0	3	2	0	0	0	1	1	0
4	0	1	1	0	3	5	0	0	1
6	6	7	5	1	8	11	2	2	3
7	1	3	3	0	1	2	7	10	1
8	0	2	3	3	2	7	4	0	1
9	5	8	16	3	8	9	11	7	5
11	6	15	8	2	8	14	7	11	2
12	2	1	1	2	2	4	0	4	3
13	4	6	8	3	13	13	6	10	1
15	4	13	18	2	13	25	8	25	0
16	4	16	12	5	18	22	16	25	4
17	2	7	9	1	17	23	7	7	2
19	3	14	7	0	7	11	7	5	1
23	1	1	4	2	11	3	1	1	2
26	0	3	4	1	4	1	2	0	0
28	5	5	2	1	2	10	1	5	4
29	19	3	7	3	12	44	7	13	4
34	3	0	4	0	15	21	10	7	2
36	16	12	33	4	27	76	15	39	1
39	1	2	7	0	2	14	4	1	0

It was also possible to successfully convert the IS-CHEC questionnaire responses into risk exposure using the participating organization's risk management framework, associated matrices, and the analysis confirmed accurate reflection of the organization's risk position with regard to human error when compared to actual incident data.

The questionnaire provided an employee perspective in that the participating organization focus was primarily driven towards quantity rather than quality of task completion, which in turn commonly results in human error and associated information security incidents. These errors would likely materialize through entering data within systems or sending of emails. The employees also put forward that they require greater training and simplification of operating procedures.

The research provides a view within this particular participating organization that it was beneficial in all 9 operational business areas to engage with staff directly to establish the actual organizational and contextual issues that could affect their ability to successfully complete intended work tasks and could result in information security incidents. Therefore, the information security community should look to adopt a mechanism for staff to freely provide them with the actual constraints to successful work task completion. This would enable the organization to implement controls to reduce the proportions of human error and associated information security incidents and breaches.

The research and the proactive use of the IS-CHEC technique in questionnaire form supports the approach taken by other questionnaires [47], [49] as outlined earlier within this paper. However, this research has shown that there are significant benefits in a specific focus on unintentional human error, links with HRA as used in the safety field, providing employees with the opportunity to suggest which systems and processes are most likely to be affected and the preventative measures which could reduce the likelihood of human error-related information security incidents occurring.

The research was limited in that the CHECs offered to employees were restricted to those experienced by participating organizations within our wider research. The benefits were ease of questionnaire completion and higher response rates but this may have potentially prevented wider themes and patterns being unearthed.

VI. CONCLUSION

In conclusion, the research has confirmed that IS-CHEC in questionnaire form was successfully applied within a

TABLE 10. GISATs by business area.

GISAT	Business Area								
	A	B	C	D	E	F	G	H	I
1	14	7	31	3	19	14	27	28	5
2	29	31	43	10	49	90	29	44	6
3	4	3	6	1	11	19	6	6	0
4	3	3	6	0	3	5	6	4	1
5	9	12	17	5	18	33	12	21	4
6	0	0	1	0	1	10	0	1	0
7	1	1	1	0	3	2	1	0	0
8	6	16	4	1	5	17	7	11	1
9	1	8	4	1	10	8	5	8	5
10	5	3	8	3	10	48	2	4	0
11	9	13	19	6	18	21	12	16	3
12	2	7	2	0	8	12	4	7	1
13	2	1	2	1	1	5	2	1	0
14	1	3	2	0	5	1	3	1	1
15	1	1	1	0	2	1	0	0	0
16	3	7	8	1	5	15	8	5	0

participating private sector healthcare organization with a focus on information security. The technique delivered proactively to the people that are subject to human error within an organization can give them a voice in order to accurately steer their employer to recognize common organizational context that negatively affects their ability to perform required tasks successfully.

The approach taken within this research shows the value of both introducing HRA as applied within the safety field and also, that a distributed approach for information security human error assessment can be successfully undertaken across a large organization. This approach can add beneficial value to organizations as an enhancement to standard information security assessment approaches where it is known that the majority of information security incidents are as a result of human error.

The results of this study show that organizational focus on its people and their working environment can improve information security understanding. This increased understanding would enable an organization to subsequently decrease the volumes of associated information security incidents through a reduction in human error. As a result of this research the participating organization was able to instigate a broad programme of improvement relating to training, standardization of documented operating procedures, recruitment and health and wellbeing initiatives such as mindfulness sessions for all staff to attend.

Future planned work includes the completion and publication of a 12 month real-time incident analysis empirical action research study across 2 participating public and private sector organizations to evaluate the effectiveness of the IS-CHEC information security human reliability analysis technique. The study, through intervention, is intended to gauge if the IS-CHEC technique when embedded within organizational practices can lead to a greater understanding of the causes and proportions of human error as well as reducing the volumes of human error-related information security incidents.

APPENDIX

A. IS-CHEC QUESTIONNAIRE INTRODUCTORY TEXT

[Redacted participating organization name] is continuously working to improve our information governance and security practices to ensure the data we process is done so securely to protect the people whose data we process every day.

We understand that the greatest asset to our organization are our people and we want to ensure you are given the opportunity to tell us anonymously of areas where we may be able to offer you the best possible support in order to prevent future incidents from occurring.

Therefore we would like you to complete the short questionnaire below. The questionnaire should take no longer than 5 minutes to complete and all answers will be treated in confidence.

B. IS-CHEC QUESTIONNAIRE DATA CAPTURE ELEMENT

See Table 7.

C. IS-CHEC QUESTIONNAIRE ANALYSIS ELEMENT

See Table 8.

TABLE 11. RPMs by business area.

RPM	Business Area								
	A	B	C	D	E	F	G	H	I
0	0	0	0	0	0	0	0	0	0
1	16	28	44	2	28	60	18	38	4
2	4	15	26	3	19	18	13	15	2
3	4	2	4	0	3	4	3	4	0
4	18	7	11	7	12	19	12	15	0
5	6	9	17	4	12	22	7	17	3
6	7	9	14	0	8	30	9	12	3
7	5	8	4	1	9	14	6	13	4
8	4	6	5	0	8	8	8	6	2
9	2	2	1	1	2	3	2	2	2
10	2	4	2	0	10	19	6	12	0
11	1	3	3	0	7	19	3	1	2
12	6	6	8	4	4	32	9	7	2
13	7	9	8	2	14	12	7	2	3
14	5	0	3	1	4	3	3	3	0
15	0	3	6	0	1	14	2	3	0
16	2	3	4	3	9	22	5	7	1
17	0	0	1	0	0	4	3	0	0
18	6	4	2	2	7	7	3	7	1
19	0	2	1	1	0	1	1	2	0
20	0	1	2	1	1	3	4	3	0
99	0	0	0	0	0	0	0	0	0

D. CHECs BY BUSINESS AREA

See Table 9.

E. GISATs BY BUSINESS ARE

See Table 10.

F. RPMs BY BUSINESS ARE

See Table 11.

ACKNOWLEDGMENT

The authors thank the editors and the anonymous reviewers for their constructive comments. The authors would also like to thank the participating organizations for their participation in the research study. The funder C. Luo had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript. The research content will be retained in accordance with the De Montfort University Research Records Retention Policy.

REFERENCES

[1] K. Renaud and S. Flowerday, "Contemplating human-centred security & privacy research: Suggesting future directions," *J. Inf. Secur. Appl.*, vol. 34, pp. 76–81, Jun. 2017.

[2] G. Bunker, "Technology is not enough: Taking a holistic view for information assurance," *Inf. Secur. Tech. Rep.*, vol. 17, nos. 1–2, pp. 19–25, Feb. 2012.

[3] M. Eminağaoğlu, E. Uçar, and Ş. Eren, "The positive outcomes of information security awareness training in companies—A case study," *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 223–229, Nov. 2009.

[4] B. Hauer, "Data and information leakage prevention within the scope of information security," *IEEE Access*, vol. 3, pp. 2554–2565, 2015.

[5] A. Jones, "How do you make information security user friendly?" *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 213–216, Nov. 2009.

[6] H. Abrar, S. J. Hussain, J. Chaudhry, K. Saleem, M. A. Orgun, J. Al-Muhtadi, and C. Valli, "Risk analysis of cloud sourcing in healthcare and public health industry," *IEEE Access*, vol. 6, pp. 19140–19150, 2018.

[7] A. J. Varela-Vaca, L. Parody, R. M. Gasca, and M. T. Gomez-Lopez, "Automatic verification and diagnosis of security risk assessments in business process models," *IEEE Access*, vol. 7, pp. 26448–26465, 2019.

[8] X.-Y. Cheng, Y.-M. Wang, and Z.-L. Xu, "Risk assessment of human error in information security," in *Proc. Int. Conf. Mach. Learn.*, 2006, pp. 3573–3578.

[9] S. M. Furnell, N. Clarke, A. Komatsu, D. Takagi, and T. Takemura, "Human aspects of information security," *Inf. Manage. Comput. Secur.*, vol. 21, no. 1, pp. 5–15, Mar. 2013.

[10] S. M. Furnell, N. Clarke, and D. Lacey, "Understanding and transforming organizational security culture," *Inf. Manage. Comput. Secur.*, vol. 18, no. 1, pp. 4–13, Mar. 2010.

[11] A. Hals, "Well integrity assessment?: Challenges related to human and organizational factors—The case study of veslefrikk," NTNU, 2015.

[12] K. Saarelainen and M. Jantti, "Quality and human errors in IT service infrastructures—Human error based root causes of incidents and their categorization," in *Proc. 11th Int. Conf. Innov. Inf. Technol. (IIT)*, Nov. 2015, pp. 207–212.

[13] H.-C. Lee, T.-I. Jang, and K. Moon, "Anticipating human errors from periodic big survey data in nuclear power plants," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 4777–4778.
[14] M. G. Lee, "Securing the human to protect the system: Human factors in cyber security," in *Proc. 7th IET Int. Conf. Syst. Saf., Cyber Secur. Conf.*, 2012, p. 41.
[15] H. E. Kim, H. S. Son, B. G. Kim, J. Cho, S. M. Shin, and H. G. Kang, "Input-domain software testing for failure probability estimation of safety-critical applications in consideration of past input sequence," *IEEE Access*, vol. 6, pp. 8440–8451, 2018.
[16] M. Alaskar, S. Vodanovich, and K. N. Shen, "Evolvement of information security research on employees' behavior: A systematic review and future direction," in *Proc. 48th Hawaii Int. Conf. Syst. Sci.*, Jan. 2015, pp. 4241–4250.
[17] J. Rajamaki, J. Nevmerzhitskaya, and C. Virág, "Cybersecurity education and training in hospitals: Proactive resilience educational framework (prosilience EF)," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Apr. 2018, pp. 2042–2046.
[18] N. R. Samaranayake, S. T. D. Cheung, W. C. M. Chui, and B. M. Y. Cheung, "Technology-related medication errors in a tertiary hospital: A 5-year analysis of reported medication incidents," *Int. J. Med. Inform.*, vol. 81, no. 12, pp. 828–833, Dec. 2012.
[19] L. Coles-Kemp, "Information security management: An entangled research challenge," *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 181–185, Nov. 2009.
[20] J. Burleigh and M. Greenfield, "Directorate/programme NHS digital external IG delivery project IG incident reporting document reference project manager status final owner annual information governance (IG) incident trends (2015–2016)," 2015.
[21] M. Evans, Y. He, L. Maglaras, and H. Janicke, "HEART-IS: A novel technique for evaluating human error-related information security incidents," *Comput. Secur.*, vol. 80, pp. 74–89, Jan. 2019.
[22] M. Evans, Y. He, L. Maglaras, I. Yevseyeva, and H. Janicke, "Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector," *Int. J. Med. Inform.*, vol. 127, pp. 109–119, Jun. 2019.
[23] M. Evans, Y. He, I. Yevseyeva, and H. Janicke, "Published incidents and their proportions of human error," *Inf. Comput. Secur.*, vol. 27, no. 3, pp. 343–357, 2019.
[24] M. Evans, Y. He, I. Yevseyeva, and H. Janicke, "Analysis of published public sector information security incidents and breaches to establish the proportions of human error," in *Proc. 12th Int. Conf. Hum. Aspects Inf. Secur. Assurance (HAISA)*, Sep. 2018, pp. 911–921.
[25] R. Vaidya, "Cyber security breaches survey 2019," 2019.
[26] C. Colwill, "Human factors in information security: The insider threat—Who can you trust these days?" *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 186–196, Nov. 2009.
[27] R. Klahr, J. N. Shah, P. Sheriffs, T. Rossington, and G. Pestell, "Cyber security breaches survey 2017," 2017.
[28] M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4667–4679, Nov. 2016.
[29] T. Gu, L. Li, M. Lu, and J. Li, "Research on the calculation method of information security risk assessment considering human reliability," in *Proc. 10th Int. Conf. Rel., Maintainab. Saf. (ICRMS)*, 2014, pp. 457–462.
[30] S. Taniuchi, T. Aoyama, H. Asai, and I. Koshijima, "Training cyber security exercise facilitator: Behavior modeling based on human error," in *Proc. Int. Conf. Appl. Hum. Factors Ergonom.*, 2019, pp. 138–148.
[31] S. M. Furnell, N. Clarke, R. Werlinger, K. Hawkey, and K. Beznosov, "An integrated view of human, organizational, and technological challenges of IT security management," *Inf. Manage. Comput. Secur.*, vol. 17, no. 1, pp. 4–19, Mar. 2009.
[32] J. T. Reason, *Human Error*. Cambridge, U.K.: Cambridge Univ. Press, 1990.
[33] L. Hadlington, M. Popovac, H. Janicke, I. Yevseyeva, and K. Jones, "Exploring the role of work identity and work locus of control in information security awareness," *Comput. Secur.*, vol. 81, pp. 41–48, Mar. 2019.
[34] I. Hwang, D. Kim, T. Kim, and S. Kim, "Why not comply with information security? An empirical approach for the causes of non-compliance," *Online Inf. Rev.*, vol. 41, no. 1, pp. 2–18, Feb. 2017.
[35] A. da Veiga and N. Martins, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," *Comput. Secur.*, vol. 49, pp. 162–176, Mar. 2015.
[36] L. Cilliers, "Exploring information assurance to support electronic health record systems," in *Proc. IST-Africa Week Conf. (IST-Africa)*, May 2017, pp. 1–8.
[37] S. Mamonov and R. Benbunan-Fich, "The impact of information security threat awareness on privacy-protective behaviors," *Comput. Hum. Behav.*, vol. 83, pp. 32–44, Jun. 2018.
[38] K. Singh, "Lifting the lid on root cause analysis: A document analysis," *Saf. Sci.*, vol. 107, pp. 109–118, Aug. 2018.
[39] J. C. Williams, "A user manual for the HEART human reliability assessment method," DNV Technica, 1992.
[40] M. Kyriakidis, V. Kant, S. Amir, and V. N. Dang, "Understanding human performance in sociotechnical systems—Steps towards a generic framework," *Saf. Sci.*, vol. 107, pp. 202–215, Aug. 2018.
[41] J. C. Williams and J. L. Bell, "Consolidation of the error producing conditions used in the human error assessment and reduction technique (heart)," *Saf. Rel.*, vol. 35, no. 3, pp. 26–76, Dec. 2015.
[42] V. Frederic and J. Victor, "The amazing human factors and their dissonances for autonomous cyber-physical & human systems," in *Proc. IEEE Ind. Cyber-Phys. Syst. (ICPS)*, May 2018, pp. 597–602.
[43] T. Kelley, M. J. Amon, and B. I. Bertenthal, "Statistical models for predicting threat detection from human behavior," *Frontiers Psychol.*, vol. 9, p. 466, Apr. 2018.
[44] R. McEvoy and S. Kowalski, "Beyond training and awareness: From security culture to security risk management," in *Proc. CEUR Workshop*, 2107, pp. 71–86.
[45] P. Mayer, A. Kunz, and M. Volkamer, "Reliable behavioural factors in the information security context," in *Proc. 12th Int. Conf. Availability, Rel. Secur. (ARES)*, 2017, pp. 1–10.
[46] L. Connolly, M. Lang, J. Gathegi, and J. D. Tygar, "The effect of organisational culture on employee security behaviour: A qualitative study," in *Proc. HAISA*, 2016, pp. 33–44.
[47] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, May 2014.
[48] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, May 2017.
[49] P. B. Goodliff and A. J. Widdowson, "CHEAT, an approach to incorporating human factors in cyber security assessments," in *Proc. 10th IET Syst. Saf. Cyber-Secur. Conf.*, 2015, pp. 1–5.
[50] *CHEAT: An Updated Approach for Incorporating Human Factors in Cyber-Security Assessments*, Thales, La Défense, Paris, 2017.
[51] NHS Digital. (2017). *NHS Information Governance Toolkit*. Accessed: Oct. 13, 2017. [Online]. Available: https://www.igt.hscic.gov.uk/
[52] *Information Security Management Systems—Requirements*, document ISO/IEC 27001, BSI, 2013.

MARK EVANS is currently pursuing the Ph.D. degree in information security with De Montfort University. He is an information security professional with over 15 years of information security experience. He has experience in designing and implementing information security management systems and frameworks within private and public sector organizations across the world. He has helped a number of organizations to understand and address their information security risks and weaknesses ranging from technical cyber security through to human factors and behavior. His research interest includes the human factors of information security with a specific focus on human error.

YING HE received the Ph.D. degree in computer science from Glasgow University, U.K. She is currently a Senior Lecturer of computer science with the School of Computer Science and Informatics, De Montfort University, U.K. Her research interests include cyber threat intelligence, security risk management, decision-making, business analytics, control systems architecture, and human's aspects of security. She also looks at how security management frameworks can be applied in different industries, such as healthcare and finance.

CUNJIN LUO received the Ph.D. degree in computer science from the Harbin Institute of Technology (HIT), China. He had also been a joint Ph.D. student with The University of Manchester. He is currently an Associate Professor with the Key Lab of Medical Electrophysiology, Ministry of Education, Southwest Medical University, China. He is also an Associate Professor with the School of Computer Science and Engineering, Northeastern University, China. His research focuses on healthcare informatics, cardiac electrophysiology, and medical data analytics. He received the National Natural Science Foundation of China (NSFC) Grant on computer modeling and healthcare diagnosis, and an Anti-poverty Project in the sustainability of health and wellbeing.

IRYNA YEVSEYEVA is a Senior Lecturer in computing science and cyber security with the Faculty of Technology, De Montfort University, Leicester, U.K., since February 2016, where she is also a member of Cyber Technology Institute. Her research interests include multicriteria decision analysis and optimization and their application in various domains including security, manufacturing, and health care and chemo-informatics. Prior to joining DMU, she was a leading Research Associate in Choice Architecture for Information Security (ChAISe) project at Newcastle University, U.K., a part of first Research Institute on Science of Cyber Security (RISCS), where she was involved in models of influencing security behaviors.

HELGE JANICKE received the Ph.D. in computer science, in 2007. He is the Technical Director of the De Montfort University's Cyber Technology Institute, where he is currently the Head of the School of Computer Science and Informatics. He worked on Cyber Security with organizations, such as Airbus, BT, QinetiQ, Ministry of Defense, and General Dynamics U.K.. His research interests include formal verification techniques and their application to cyber security, SCADA and industrial control system security as well as aspects of cyber warfare. He established DMU's Airbus Group Centre of Excellence in SCADA Cyber Security and Forensics Research, in 2013. He is the General Chair of the International Symposium on SCADA and Industrial Control Systems Cyber Security Research (ICS-CSR). He serves on the Editorial Board and as a Reviewer for a number of international journals.

LEANDROS A. MAGLARAS received the B.Sc. degree from the Aristotle University of Thessaloniki, Greece, in 1998, the M.Sc. degree in industrial production and management from the University of Thessaly, in 2004, the M.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Volos, in 2008 and 2014, respectively, and the Ph.D. degree in intrusion detection in SCADA systems from the University of Huddersfield, in 2018. He is currently the Director of the National Cyber Security Authority of Greece and a part-time Senior Lecturer with the School of Computer Science and Informatics, De Montfort University, U.K. He has authored more than 100 papers in scientific magazines and conferences.