Received August 21, 2019, accepted September 23, 2019, date of publication September 30, 2019, date of current version October 10, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2944615

Real-Time Information Security Incident Management: A Case Study Using the IS-CHEC Technique

MARK EVANS[1], YING HE[1], CUNJIN LUO[2,3], IRYNA YEVSEYEVA[1], HELGE JANICKE[1], EFPRAXIA ZAMANI[4], AND LEANDROS A. MAGLARAS[1]

[1]Cyber Technology Institute, 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
[4]Information School, University of Sheffield, Sheffield S10 2TN, U.K.

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

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

ABSTRACT Information security recognised the human as the weakest link. Despite numerous international or sector-specific standards and frameworks, the information security community has not yet adopted formal mechanisms to manage human errors that cause information security breaches. Such techniques have been however established within the safety field where human reliability analysis (HRA) techniques are widely applied. In previous work we developed Information Security Core Human Error Causes (IS-CHEC) to fill this gap. This case study presents empirical research that uses IS-CHEC over a 12 month period within two participating public and private sector organisations in order to observe and understand how the implementation of the IS-CHEC information security HRA technique affected the respective organisations. The application of the IS-CHEC technique enabled the proportions of human error related information security incidents to be understood as well as the underlying causes of these incidents. The study captured the details of the incidents in terms of the most common underlying causes, selection of remedial and preventative measures, volumes of reported information security incidents, proportions of human error, common tasks undertaken at the time the incident occurred, as well as the perceptions of key individuals within the participating organisations through semi-structured interviews. The study confirmed in both cases that the vast majority of reported information security incidents relate to human error, and although the volumes of human error related incidents pertaining to both participating organisations fluctuated over the 12 month period, the proportions of human error remained consistently as the majority root cause.

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

I. INTRODUCTION

The field of information security has developed numerous standards and frameworks governing how information should be processed by organisations. These standards include the ISO27000 series [1], Payment Card Industry Data Security Standard [2] and also sector specific policies and standards such as the Data Security and Protection Toolkit [3] applied to the National Health Service in Britain. Despite numerous international and sector-specific standards and frameworks, the information security community has not adopted a formal mechanism to deal with human errors, such as the application of human reliability analysis (HRA) techniques [4], [5] which are widely used in high reliability sectors [6].

In previous work we demonstrated that human errors account for the majority of incidents [7]. These incidents pertain frequently to unintentional human error compared to intentional and possibly malicious action, technology failings, procedural failings or weaknesses in physical controls [7]–[9], and are still occurring without resulting in any key

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

changes to common organisation practices to address these issues. People are susceptible to slips and lapses [10], which can affect the accuracy of tasks and often result in information security incidents. Yet despite this well understood limitation of workers, we identified that there is a comparative lack of prevention techniques and literature related to unintentional human error in information security assurance when compared to technology vulnerability or malicious intent including insider threat as outlined later in this paper.

As part of our broader research into information security related human error, we have undertaken and published related research which proactively applies the IS-CHEC technique [11]. This research uses a questionnaire delivered to operational employees [11] rather than information security professionals acting reactively to reported incidents. The proactive use of IS-CHEC was applied within the same private sector organisation as applied within this article and provides an employee's perspective on human error and suggested controls to enable risk quantification across the organisation to be performed.

The focus on the detection and prevention of human error in an information security setting is less established compared to high reliability sectors, such as NASA [12] where numerous HRA techniques have been evaluated and applied. It has also been established and published that with regard to human error related incidents, the human is not actually the cause of an incident but in fact the consequence of wider organisational failings [13].

This paper evaluates the application of the Information Security Core Human Error Causes (IS-CHEC) technique [8] applied to information security incident management over a 12 month period of time within participating public sector and private sector organisations simultaneously. The IS-CHEC technique is an adaptation of the Human Error Assessment and Reduction Technique (HEART) which has been in use for 30 years within industries such as rail, aviation, nuclear and healthcare to address the human error issue [14]. The HEART HRA technique was selected as the most applicable to an information security setting due to its accuracy, compatibility, needed resources, output and comprehensiveness [9]. The IS-CHEC technique was embedded within the information security incident management practices, as a component of our wider empirical action research to establish the root cause of reported incidents and, where the root cause is identified as being unintentional human error, to delve deeper into the underlying causes, and finally, to apply a framework of remedial and preventative measures to resolve the incident and prevent a re-occurrence.

The principal motivation and research hypothesis behind this work was to establish if the IS-CHEC information security HRA technique could have a positive or negative effect on information security within public and private sector organisations. If present, this positive effect would primarily materialise through a greater understanding of the proportions and underlying causes of information security related human error. The research establishes the most common causes of information security human error related incidents within the public and private sector organisations, as well as providing valuable actionable insights into information security aspects. An additional motivation is the potential to reduce human error and, therefore, a decline in the volumes of reported information security incidents.

This paper makes the following contributions:

- Conducts real-time longitudinal empirical research simultaneously within public and private sector organisations using the IS-CHEC technique for the first time within published literature.
- Presents the volumes and proportions of human error related information security incidents, plus the association between the proportions of human error related incidents and the overall volume of information security incidents, over the course of a 12 month period of empirical research within public and private sector organisations.
- Captures and presents the underlying themes pertaining to tasks performed at the time of the incidents, underlying causes and effectiveness of remedial and preventative measures.

These contributions will benefit academia through the publication of much needed empirical research into the effects of human error within the field of information security. Moreover, the contributions will not only positively benefit industry and wider society initially through the participating organisations delivering healthcare services, but will also subsequently provide an information security human reliability technique that can be applied across multiple sectors.

This paper presents the findings of a 12 month empirical case study of the effectiveness of the IS-CHEC information security HRA technique. The case study comprised of a real-time analysis exercise within participating public and private sector organisations following on from our previous retrospective analysis case studies [9]. The research enables further accuracy and evolution of the IS-CHEC technique from previous studies due to the timely nature of investigations. This paper presents a comprehensive and detailed output in relation to information security incident management, specifically focusing on the incidents that relate to human error. Therefore, this paper presents an established and tested information security HRA which is applicable to be adopted by a wider range of areas of information security to address the current gap in knowledge and practice.

The remainder of this paper is structured as follows. Section 2 presents related information security work and associated literature. Section 3 details the research method including the case study organisations, the data capture techniques applied and also introduces the IS-CHEC information security HRA technique. Sections 4 and 5 present IS-CHEC, its adaptations, how it was implemented and the detailed results of the case study. Section 6 presents the findings, implications, comparisons with the literature and any limitations of the method and technique. Finally, section 7

captures the research conclusions and presents future work on this topic.

II. RELATED WORK

A literature search was performed on 26/01/2019 using the SCOPUS abstract and citation database for any article published in 2019 using the search criteria of 'Information Security' or 'Cyber Security'. The search returned 324 articles. We reviewed the abstract for each of these documents, and the full article where further understanding was required, whereupon we established that 67 articles were not information security related. From the remaining 257 articles it was found that 6 related to unintentional human error which equates to 2%. Of these 6 articles only 1 was primarily focussed on the topic of human error within the field of information security which equates to 0.4%.

The human is recognised as being the weakest link in organisational information security controls [15]–[20], which has resulted in publications focussing on human factors rather than technical aspects [16]. This is due to humans not behaving securely when using systems [18] which makes them a significant information security threat facing organisations [16]. However, with appropriate controls applied, the human can transform from the weakest link to the strongest link [19].

Previous research [9] defines a human error related information security incident as an 'active failure' by a person (the threat) performing an 'intentional action' resulting in the failure to complete a task as intended or achieve the desired outcome due to the exploitation of a 'latent condition' (the vulnerability). This can lead to a compromise or breach of information confidentiality, integrity or availability or associated law through the failure of technical or organisational safeguards, and can cause disruption to business operations or causing harm or distress to individuals including breaches of privacy.

Stewart and Jurjens [21] presented in their research an empirical study which had found that 65% of data breaches were due to loss of paper files and human carelessness. Alavi *et al.* [22] presented similar findings, in which 64% of security incidents are directly related to human error. Further research presented by Asai and Hakizabera [23] suggests that 80% of information security breaches are caused by human error.

The Cyber Security Breaches Survey [24] states that human error is amongst the most common factors contributing to the most disruptive breaches, indicating that human error is not only exposing organisations to the majority of incidents, but also that those are the most impacting. Veiga and Martins [25] refer to surveys and research conducted by PriceWaterHouse and Ponemon Institute that established that 58% and 35% respectively of information security incidents and breaches were attributable to human factors, although they do not differentiate between intentional violations and unintentional human error. To add to this, Hwang *et al.* [26] refer to external reports, which presented that 14% of information exposures originated from organisational insiders.

The human factor is one of the most vulnerable aspects of cyber security incidents [27], and as set out in literature, the human factor is a most important component of information security, perhaps more important than the technical measures [28]. Human activity is the most critical factor in the management of information security [21] with experts growingly arguing that the main cause of information security incidents mainly lies with employees' behavioural factors rather than technical issues [29]. It was presented by Rajamäki *et al.* [30] that employee negligence was a greater concern to healthcare organisations than cyber-attack.

There also appears within information security literature generally that there is a much greater focus on the human factors being as a result of intentional action or attacks [31] rather than unintentional human error, such as the 2017 Data Breach Investigations Report [32].

Organisations should develop strategies to reduce information security threats by employees [26] including focussing on employees' behaviour [17]. Health Information Systems require rigorous evaluation that addresses human issues in addition to technology and organisational issues [33], which should lead to cultural change [34] and the implementation of system designs, which will display warning messages when user mistakes are made and prevent them from completing a task [35].

In addition to proactive and strategic planning, retrospective analysis of incidents is important and can include root cause analysis, which is oriented to the identification of data associated with a specific occurrence [36]. Information security management remains relatively weak in conducting root cause analysis of minor incidents [37]. HRA can be used to both support retrospective and predictive analysis, but when applied to new fields this will have to be empirically derived [38].

III. RESEARCH METHOD

This research is based upon empirical research within participating organisations to drive information security improvements and forms part of a wider programme of action research study.

Action research is concerned with exploring and challenging real life situations within organisational settings in order to solve problems through intervention [39]. It also generates new knowledge which is useful for both research and practice [40]. The research is based upon practical application to offer a solution to the problem of current information security incidents occurring as a result of human error.

The research adopted participatory research within the participating organisation settings in order to observe and ascertain how the introduction of HRA techniques in an information security environment affects the respective organisations.

A. RESEARCH SITES

The case study benefitted from two participating organisations. One organisation was a public sector body and the other was a private sector organisation. Both organisations provide healthcare services to the British National Health Service (NHS) and, therefore, provide a reflective sample covering public and private sector organisations. They also provide insight into healthcare providers, which suffer from a large proportion of information security incidents and breaches related to human error [7].

The public sector organisation has approximately 2,000 employees and provides a range of services. Its incident management practices are required to support compliance with legislation and government guidance. Information security is governed centrally by the Head of Security and Information Assurance and their small team, who are responsible for the development of organisational strategy and policy as well as oversight and engagement in all reported incidents. Designated individuals, usually managers, within each business area have responsibility for information security application in addition to their primary role. These Business area representatives are not dedicated information security professionals, but attend formal governance sessions with the information security team on a bi-monthly basis. The organisation has an information security policy as well as an information security incident policy and procedures in place, which are communicated to all employees as part of annual awareness requirements. Compliance in terms of awareness are continuously monitored and acted upon.

The private sector organisation is a large service provider operating in the United Kingdom. It has approximately 1,100 employees and provides a range of services to the NHS. 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. Information security is governed centrally by the Senior Information Risk Owner and associated team, who are responsible for the development of organisational strategy and policy. In addition, designated information security leads have responsibility for every business area to ensure full coverage and adherence.

B. DATA COLLECTION AND ANALYSIS

We used semi-structured interviews and document reviews as data capture techniques and instruments over a 12 month period with both participating organisations simultaneously as they applied the IS-CHEC technique. The research began with the establishment of a researcher-client agreement [39], which included ensuring a common understanding of the research background, problem and intended solution. The agreement also formalised objectives and clear responsibilities for the participating organisation and researcher. Finally, the agreement set out the duration of the research which was agreed to be a minimum of 6 months, with the option for the participating organisation to extend to 12 months. Both organisations elected after 6 months to extend the research to cover the full 12 month period. The research adhered to De Montfort University (DMU) ethical standards and guidelines, and has been approved by the DMU ethics committee (ref: 1516/325).

The research required the organisations to review their respective incident management documentation and systems to fully incorporate the IS-CHEC technique prior to beginning the case study. Once the research had begun, a formal monthly incident management meeting, which was already in operation within both organisations, was expanded to include a comprehensive IS-CHEC report as a standard agenda item. The report was initially compiled and presented by the researcher using a monthly incident register extract supplied by the organisations each month. The organisations took responsibility for report compilation and presentation from month 10 upon mutual agreement. The report template can be seen in the Appendices.

At the end of the research, semi-structured interviews were undertaken with key individuals responsible for information security and incident management as well as senior management within both organisations. The interviews were face to face, scheduled for one hour and digitally recorded. The interviews were subsequently transcribed, data coded and thematically analysed using NVivo version 11 software. Within both organisations it was important to interview personnel responsible for using IS-CHEC, but also senior managers in both organisations to gather their views and opinions. Therefore, within the public sector organisation we interviewed the Head of Security and Information Assurance (HoS&IA), Head of Internal Governance, who was also the Deputy Senior Information Risk Owner (Deputy SIRO) and Information Security Manager (ISM). The ISM was responsible for the implementation of IS-CHEC. Within the private sector organisation, we interviewed the Chief Operating Officer (COO), Senior Information Risk Owner (SIRO), Information Security Manager (ISM) and Information Security Incident Analyst. The ISM and Information Security Incident Analyst were responsible for the implementation of IS-CHEC. The interviewees were asked to read and sign an informed consent form and asked to describe their role in the organisation, their responsibilities and the tasks or activities they are involved in and how this integrates with wider organisational information security. The interviewees were then asked the seven questions listed below in order to capture contextual qualitative information to ascertain their respective perceived applicability and effects of IS-CHEC on their role and organisation, any new learning, any overall thoughts on the study and finally their understanding of the underlying causes of information security related human error which would support the principal motivation behind the study.

- Could you explain your understanding of the IS-CHEC technique, the engagement you have had with the technique and what impact this has had on your role?
- Do you feel that the IS-CHEC technique, and its components, such as GISAT and CHEC, is applicable for an information security implementation?

Please expand upon your response with as much detail as possible.

- Tell me about the positive effects, if any, that IS-CHEC has had on the organisation? Please expand upon your response and provide positive examples if there are any.
- Throughout the course of the IS-CHEC information security incident project, what would you say have been the greatest challenges? Please expand upon your response with examples if possible.
- Through the use of IS-CHEC have you learned anything new about your organisation and its people in terms of behaviours relating to information security? Please expand on your response.
- On reflection, would you suggest any changes to the organisation, approach taken, or the IS-CHEC technique? Please provide the rationale behind your suggested changes.
- Do you have any other opinions or feelings about the IS-CHEC information security incident project that you would like to share?

To establish if there was a linear relationship between the proportions of human error related information security incidents and the overall volume of information security incidents, we applied Pearson's Correlation Coefficient using the formula presented below. The variable 'x' relates to the total number of incidents and 'y' relates to the number of human error-related incidents. We then compared the results attained for both organisations. The output is known as the r coefficient.

$$r = \frac{\sum_{i=1}^{n}((x_i - \bar{x})(y_i - \bar{y}))}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} \quad (1)$$

The output from this formula is in the form of statistical ranges from +1 through 0 to −1. A result of +1 would identify a perfect positive correlation, 0 would identify that there was no correlation and −1 would identify a perfect negative correlation. As set out by Taylor [41], a result of <=0.35 would be interpreted as a weak correlation, 0.36 – 0.67 would be interpreted as a modest correlation and 0.68 – 1.0 would be interpreted as a strong correlation.

In order to ensure research rigor in terms of validity and reliability, a number of mechanisms were embedded throughout the duration of the research. These methods aligned to the four criteria for research validity and reliability, [42]–[44] comprising of construct validity, internal validity, external validity and reliability. This was primarily achieved through the application of semi-structured interviews, routine formal governance within each participating organisation including a review of all incidents and the monthly IS-CHEC report, agreement and application of clear research objectives as part of the signed researcher-client agreement and also the strict application of the IS-CHEC technique to provide demonstrable cause and effect data related to human error related information security incidents. Our findings were constantly interpreted and reviewed in light of existing literature and in consultation with the two participating public and private sector organisations, to ensure that they are consistent and that they accurately reflect the actual events. In addition, the research was undertaken and compared within the two participating organisations simultaneously and the required research material, including the IS-CHEC technique, methods and results, to enable the research to be replicated has been published in this article and prior articles relating to our work [7]–[9], [11], [45], [46].

IV. IMPLEMENTATION

In this section we present a high-level introduction to the IS-CHEC technique and also the further adaptations that have been made to the technique over the course of the case study.

A. IS-CHEC INTRODUCTION/OVERVIEW

The IS-CHEC technique is an adapted version of the HEART technique that is split into two elements, which have been presented in our previous work [8]. These are an IS-CHEC mapping element and an analysis element. The mapping element was appended to the participating organisations' incident registers to enable all recorded incidents to be analysed and acted upon using IS-CHEC in terms of its components such as General Information Security Affecting Tasks (GISAT), Core Human Error Causes (CHEC), CHEC Weighting or Significance (WoS) and Remedial and Preventative Measures (RPM). RPMs are mapped to the identified CHECs for each incident to enable consistent and effective incident management. The IS-CHEC analysis element was a separate tool from the mapping tool, which comprised of a number of fields, which were used in order to allow the HEART in-built likelihood calculations to be analysed against actual incident likelihoods as part of the monthly IS-CHEC report. The GISATs shown in Table 1 were mapped to a primary HEART Generic Task Type (GTT) and associated nominal likelihood of failure. As it was found that the context of a GISAT being performed could affect the GTT mapping, alternate mappings were also captured. The complete list of CHECs and results can be seen in Tables 5 and 6 which is an expansion of the original HEART Error Producing Conditions (EPC) [8], [47]. The full list of RPMs and their associated measure of effectiveness, plus their results, can be seen in Table 7. The IS-CHEC technique process flow is shown in Figure 1 as applied to every reported information security incident. This was required to be applied for every reported incident. Both organisations applied quality assurance processes to ensure incidents were investigated and that the associated investigation reports were accurate. Both organisations made it clear that they expected employees to report information security incidents immediately. They also both independently set expectations that all information security incidents would have the root cause analysis completed plus the identification of IS-CHEC components and associated remedial and preventative measures within 5 working days. There was no

TABLE 1. GISAT mapping to the HEART Generic Task Types (GTT) [47].

GISAT	HEART GTT Mapping	Alternate GTT Mapping
GISAT1- Sending an email	G	D
GISAT2 - Entering, updating or deleting data within a system, file or document	D	E, G
GISAT3 - Posting an item or information	E	D, G
GISAT4 - Configuring a system	B	A, C, F
GISAT5 - Administering a system	D	F, G
GISAT6 - Scanning a document	D	E, G
GISAT7 - Printing a document	D	E, F
GISAT8 - Providing information verbally	G	D
GISAT9 - Delivering information or equipment	G	D
GISAT10 - Filing or sorting information	G	E, D
GISAT11 - Reading or checking an email, file, document or item	G	A, C, D, E
GISAT12 - Safeguarding information or equipment	G	D, E
GISAT13 – Destroying information or equipment	D	A, E, G
GISAT14 – Accessing a location or environment	G	
GISAT15 – Faxing information	D	E, G
GISAT16 - Sharing or handing over information or equipment in person	G	

expectation that all incidents would be fully closed within a set timeframe although progress was continuously monitored. The five root cause options applied as part of the case study, and their results, can be seen in Tables 2 and 3. As per the process shown in Figure 1, the IS-CHEC technique is only applied where the root cause is identified to be a human error. However, the capturing of all root cause options was useful for the participating organisations in terms of trend analysis.

B. FURTHER ADAPTATION OF IS-CHEC

Over the course of the 12 month case study there were ongoing reviews undertaken of the IS-CHEC technique and the impact it was having each month as part of the respective organisations' incident management meetings. The changes that have been applied to the IS-CHEC technique, as a result of ongoing evaluation throughout the case study since it was last published in literature [8], included the establishment of a standard IS-CHEC reporting format, the expansion of the GISATs to include 'faxing information' and 'sharing or handing over information or equipment in person'. Two additional CHECs were introduced for 'distraction/task interruption' and 'time of day' following a review of the HEART EPCs [14]. A mapping of CHECs to RPMs was also maintained throughout the case study. The CHEC-RPM mapping is located in the Appendix of this paper. Over the course of the study, the list of RPMs was enhanced and modified based upon monthly formal incident management meetings which included a review of all incidents and the monthly IS-CHEC report. This was intended to encourage effective selection and application of actions and support a reduction in reported incident volumes. The introduced RPMs, due to incident review with the public sector organisation, were RPM15 (split process and introduce segregation of duties), RPM19 (recover, collect or destroy information or equipment) and RPM20 (reissue or resend information or equipment). In addition, the list of RPMs was evaluated against published literature [48], [49]. This review led to additional RPMs being agreed with the participating organisations and added to the IS-CHEC technique and also, very importantly, the strength of each RPM being determined. The introduced RPMs, due to literature review, were RPM16 (eliminate or reduce distractions), RPM17 (eliminate look-and-sound-alikes) and RPM18 (introduce warnings, alerts or alarms). The literature described the strength of each action as strong, medium or weak. However, the public sector organisation was not comfortable reporting on their people applying, or selecting, 'weak' actions. Therefore, the strength wording was modified to reflect effectiveness with the 3 indicators being higher effectiveness, moderate effectiveness and lower effectiveness. The review of literature enabled gaps in the IS-CHEC technique actions to be identified and addressed as well as adopting the strength from the published literature. Other modifications, due to the literature review, were RPM5 having the term 'standardisation' being added in relation to procedures, tools, systems or practices and RPM8 incorporating audit in addition to assessment.

V. RESULTS

In this section, results are presented in terms of incident volumes and proportions of human error (sub-section A) and association between the total volumes of information security incidents and proportions of human error related incidents (sub-section B). Both are aligned to the IS-CHEC technique and its core components such as root cause, GISAT, CHEC and RPM which are presented as underlying incident themes (sub-section C). We also present the qualitative results of the semi-structured interviews held with key individuals within both organisations (sub-section D).

A. VOLUMES AND PROPORTIONS OF HUMAN ERROR RELATED INFORMATION SECURITY INCIDENTS

In this sub-section we present the total number of incidents experienced by both participating organisations as well as the percentages of human error and other root causes. The results for the public sector organisation can be seen in Table 2 and Figure 2. The private sector organisation results are presented in Table 3 and Figure 3.

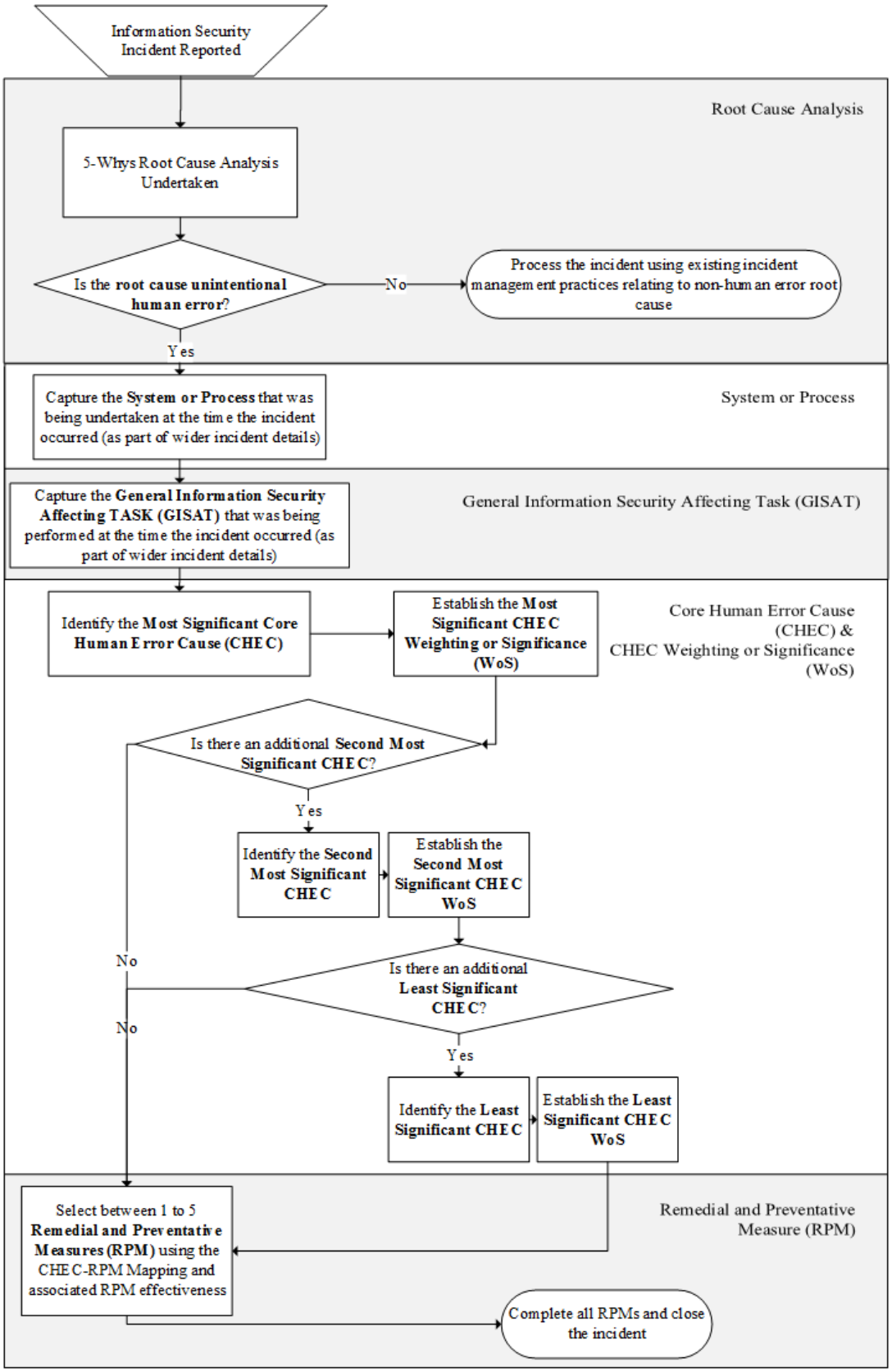


FIGURE 1. IS-CHEC incident process.

TABLE 2. Public sector incidents.

	Month												Total	%
	1	2	3	4	5	6	7	8	9	10	11	12		
Total Incidents	4	20	10	24	15	22	31	23	16	31	30	28	254	
RC1 – Human Error Slip or Lapse (Unintentional)	4	12	6	19	12	15	27	18	11	27	25	24	200	78.74
RC2 – Human Factor (Intentional Act. E.g. hacking or non-compliance with policy)	0	2	0	0	1	6	1	0	0	2	0	2	14	5.51
RC3 – Technology Failure or Configuration	0	1	2	4	2	0	3	3	4	2	4	2	27	10.63
RC4 – Procedural Mistake or failure	0	5	0	1	0	1	0	2	1	0	1	0	11	4.33
RC5 - Physical Control Failure	0	0	2	0	0	0	0	0	0	0	0	0	2	0.79
Proportion of Human Error (%)	100.00	60.00	60.00	79.17	80.00	68.18	87.10	78.26	68.75	87.50	83.87	85.71		

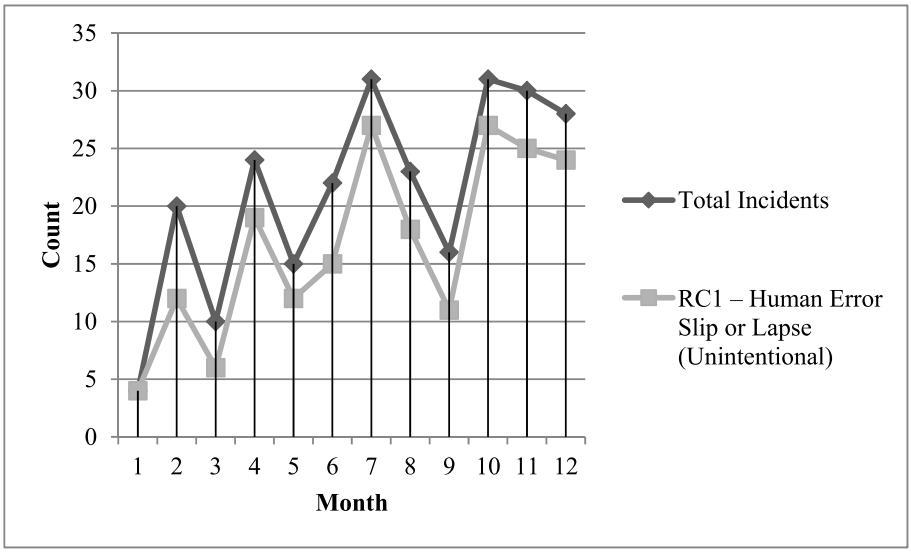


FIGURE 2. Public sector incidents and proportions of human error.

Comparison: The respective participating organisations realised differences in terms of the volumes of reported information security incidents. The public sector organisation saw an increase in reported incidents from the first month to the last month, whereas the private sector organisation saw a decrease. However, the public sector organisation did realise a reduction in incidents over the last 2 months of the study.

Both organisations recorded the fact that human error related information security incidents accounted for the majority of incidents over the duration of the study and also for every individual month.

B. LINEAR ASSOCIATION BETWEEN THE TOTAL NUMBER OF INCIDENTS AND PROPORTION OF HUMAN ERROR RELATED INCIDENTS

As outlined within the research method section, we applied Pearson's Correlation Coefficient to the total numbers of incidents and the recorded human error related incidents in order to obtain an r coefficient value. The calculations data for both organisations can be seen in Tables 23 and 24 within the Appendices.

The statistical analysis undertaken demonstrates a strong association with the public sector organisation having an r coefficient value of 0.975 and the private sector having an r coefficient value of 0.981.

Comparison: The statistical analysis has shown that both participating organisations have a strong, and similar, linear relationship between the total numbers of information security incidents and the proportions of human error related incidents over the 12 month duration of the study.

C. UNDERLYING INCIDENT THEMES

In this sub-section we present the results associated with the core IS-CHEC technique components which are used

TABLE 3. Private sector incidents.

	Month												Total	%
	1	2	3	4	5	6	7	8	9	10	11	12		
Total Incidents	45	38	30	39	52	23	23	27	8	23	28	24	360	
RC1 – Human Error Slip or Lapse (Unintentional)	44	32	29	33	49	21	19	24	8	19	27	17	322	89.44
RC2 – Human Factor (Intentional Act. E.g. hacking or non-compliance with policy)	1	3	0	1	2	0	3	2	0	3	0	3	18	5.00
RC3 – Technology Failure or Configuration	0	1	0	1	0	1	1	1	0	0	1	4	10	2.78
RC4 – Procedural Mistake or failure	0	2	0	2	1	1	0	0	0	1	0	0	7	1.94
RC5 - Physical Control Failure	0	0	1	2	0	0	0	0	0	0	0	0	3	0.83
Proportion of Human Error (%)	97.78	84.21	96.67	84.62	94.23	91.30	82.61	88.89	100.00	82.61	96.43	70.83	89.44	

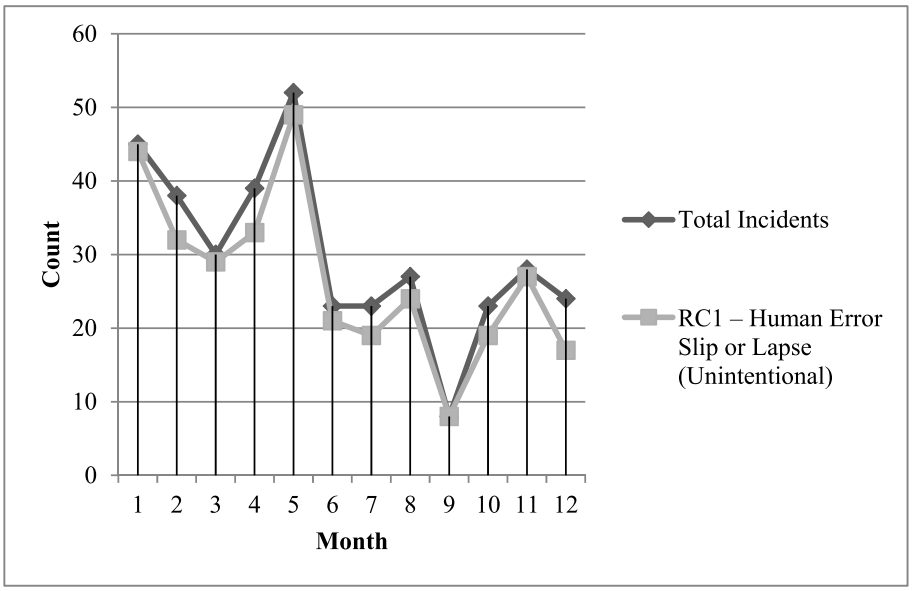


FIGURE 3. Private sector incidents and proportions of human error.

to establish the underlying details associated with reported incidents. These core components are GISAT, CHEC and RPM.

General Information Security Affecting Tasks (GISAT): The volumes of GISATs for both organisations can be seen in Table 4. The 16 GISATs are utilised to establish the actual task that was being performed at the time an incident occurred.

Comparison: There was a correlation relating to the types of tasks that were being performed when incidents occurred. Although in a different order, both organisations recorded GISATs 1, 2, 3 and 10 as part of the most common 5 GISATs providing a picture that communicating, editing or filing confidential or personal data by operational administrative personnel accounted for the vast majority of incidents.

Core Human Error Causes (CHEC): The 42 CHECs and their volumes are presented in Table 5 for the public sector organisation and Table 6 for the private sector organisation. Each time an incident was recorded, the most significant CHEC had to be recorded. The organisations were also required to capture, where appropriate, a second most significant CHEC and a least significant CHEC.

Comparison: Both organisations clearly recorded the same most common CHEC. CHEC 17 accounted for 56% of recorded public sector incidents and 33% of private sector incidents. This presents a view that both organisations detected that a lack of checks on the quality human output and human fallibility was the most common underlying cause of information security incidents.

Remedial and Preventative Measures (RPM): Each time an incident was recorded it was required that both organisations

TABLE 4. Public & Private sector GISATs.

Public Sector GISAT	Public Sector Incidents	Private Sector GISAT	Private Sector Incidents
GISAT3 - Posting an item or information	94	GISAT1- Sending an email	86
GISAT2 - Entering, updating or deleting data within a system, file or document	46	GISAT2 - Entering, updating or deleting data within a system, file or document	65
GISAT1- Sending an email	34	GISAT10 - Filing or sorting information	58
GISAT10 - Filing or sorting information	5	GISAT11 - Reading or checking an email, file, document or item	39
GISAT12 - Safeguarding information or equipment	4	GISAT3 - Posting an item or information	34
GISAT5 - Administering a system	4	GISAT9 - Delivering information or equipment	34
GISAT6 - Scanning a document	4	GISAT7 - Printing a document	2
GISAT4 - Configuring a system	3	GISAT12 - Safeguarding information or equipment	2
GISAT7 - Printing a document	2	GISAT4 - Configuring a system	1
GISAT8 - Providing information verbally	2	GISAT14 – Accessing a location or environment	1
GISAT11 - Reading or checking an email, file, document or item	1	GISAT5 - Administering a system	0
GISAT14 – Accessing a location or environment	1	GISAT6 - Scanning a document	0
GISAT13 – Destroying information or equipment	0	GISAT8 - Providing information verbally	0
GISAT15 – Faxing information	0	GISAT13 – Destroying information or equipment	0
GISAT16 - Sharing or handing over information or equipment in person	0	GISAT15 – Faxing information	0
GISAT9 - Delivering information or equipment	0	GISAT16 - Sharing or handing over information or equipment in person	0

capture at least 1 RPM. However, the organisations were able to capture up to 5 RPMs for each incident. Table 7 presents the total for each RPM captured for all incidents by both organisations and Figures 4 and 5 present the percentages of each RPM effectiveness category as applied.

Comparison: There were some key differences between the two participating organisations in terms of the selection of RPMs and their effectiveness plus the volume of actions per incident. The public sector organisation recorded 254 actions for their 200 recorded human error related information security incidents. This equates to an average of 1.27 actions for each incident. The private sector organisation recorded 645 actions for their 322 incidents, which equates to an average of 2 actions per incident.

In addition, the public sector organisation RPMs included 9% with an indicated higher effectiveness, whereas 19% of the private sector applied RPMs had a higher effectiveness.

Both the volumes of overall actions in proportion to the number of recorded incidents, and the fact that the private sector organisation applied a greater percentage of RPMs with a higher effectiveness, could have been an influential factor as to why the private sector organisation benefitted from a reduction in reported information security incidents, whereas the public sector organisation experienced an increase.

However, there were also similarities with both organisations applying RPM1, 5 and 6 as the most common three RPMs, although in a different order.

D. PARTICIPANT'S IS-CHEC UNDERSTANDING, VIEWS AND OPINIONS

As outlined earlier we undertook semi-structured interviews with participants, which comprised of seven open-ended questions. The question responses were subject to transcription, coding and thematic analysis using the NVivo version 11 software. The results are presented in Table 8.

Overall the key themes were that greater incident understanding was obtained relating to overarching incident trends and patterns as well as specific incident details such as the root cause. Another theme was that the undertaken research benefitted both organisations in the form of enhanced buy-in as a result of the used technique, which is uncomplicated, and provides quality reporting which is understandable to all stakeholders and works well.

The most common 20 words from the transcribed interviews are presented below in Table 9. In terms of themes, the adoption of the IS-CHEC technique provided themes of how it had promoted greater thought in terms of low level incident understanding and acceptance of people and their mistakes, as well as common themes around what causes these mistakes to happen. In addition, both the words 'actually' and 'know' were commonly spoken providing an indication of greater understanding of the facts relating to incidents.

In addition to the overall summary (Table 8), there is an expansion of the core themes captured through the semi-structured interviews. These core themes included that both

TABLE 5. Public sector CHECs.

CHEC	Most Significant	Second Most Significant	Least Significant	Total
CHEC17 - Little or no independent checking or testing of output	93	21	2	114
CHEC39 - Little or no self-checking or testing of output	24	2	1	27
CHEC8 - Person performing the task is monitoring numerous incoming information channels at the same time, such as numerous computer monitors	22	0	1	23
CHEC1 - Unfamiliarity with a task or situation which is potentially important but which only occurs infrequently or which is novel	19	1	0	20
CHEC3 - Too many alerts, notifications, messages or inputs leading to important information not being seen or heard and acted upon	6	4	1	11
CHEC7 - No obvious means of reversing an unintended action	6	2	0	8
CHEC11 - The person performing the task does not fully understand the policy, standards, process or procedures they are required to adhere to	4	2	0	6
CHEC12 - The person performing the task does not understand the actual risk exposure	4	2	0	6
CHEC15 - Inexperience of the person performing the task	4	2	0	6
CHEC2 - A shortage of time available for error detection and correction	3	2	0	5
CHEC13 - The system information communicated is inaccurate, unclear or inappropriate	5	0	0	5
CHEC9 - Person performing the task required to learn a new technique, process, procedure or way of working which differs in attitude or way of thinking to the previous one	3	1	0	4
CHEC29 - High-level emotional stress	3	0	0	3
CHEC28 - Person performing the task is unaware of its significance and their contribution to corporate objectives	2	0	0	2
CHEC16 - Inaccurate or incomplete information communicated by procedures or from a person to a person	1	0	0	1
CHEC23 - Unreliable instrumentation used to communicate information leading to lack of trust and person performing the task ignoring information	1	0	0	1
CHEC4 - Too easy to switch off, disable or incorrectly modify alerts, notifications, messages, or inputs leading to important information being missed or not acted upon	0	0	0	0
CHEC5 - No means of communicating information in a form which can be understood and used	0	0	0	0
CHEC6 - A mismatch between an operator's model of the world and that imagined by a designer	0	0	0	0
CHEC10 - The need to transfer specific knowledge from task to task without loss	0	0	0	0
CHEC14 - The system information which confirms that an action has been successfully completed is delayed, takes too long or does not happen	0	0	0	0
CHEC18 - A conflict between immediate and long-term objectives	0	0	0	0
CHEC19 - Not enough information to allow completeness or accuracy checks to be undertaken	0	0	0	0
CHEC20 - A mismatch between the educational achievement level of an individual and the requirements of the task	0	0	0	0
CHEC21 - An incentive to use other more dangerous procedures	0	0	0	0
CHEC22 - Little opportunity, such as rest breaks, to exercise mind and body outside the immediate confines of a job	0	0	0	0
CHEC24 - A need for decision making which is beyond the capabilities or experience of the person performing the task	0	0	0	0
CHEC25 - Unclear allocation of role and responsibility	0	0	0	0
CHEC26 - No obvious way to keep track of progress during an activity	0	0	0	0
CHEC27 - Task requirement exceeds the physical capabilities of the person performing the task	0	0	0	0
CHEC30 - Evidence of ill-health amongst operatives, especially fever	0	0	0	0

TABLE 5. *(Continued.)* **Public sector CHECs.**

CHEC	Most Significant	Second Most Significant	Least Significant	Total
CHEC31 - Low workforce morale	0	0	0	0
CHEC32 - Information displayed and how this is applied within procedures or working practices is not fully understood	0	0	0	0
CHEC33 - A poor or hostile environment (below 75% of health or life-threatening severity)	0	0	0	0
CHEC34 - Prolonged inactivity or highly repetitious low mental workload tasks	0	0	0	0
CHEC35 - Disruption of normal work-sleep cycles	0	0	0	0
CHEC36 - Pressure from someone else to increase the speed or pace at which a task is performed, beyond an individual's preferred pace and capability	0	0	0	0
CHEC37 - Additional team members over and above those necessary to perform task normally and satisfactorily	0	0	0	0
CHEC38 - Age of personnel performing perceptual tasks requiring the ability to interpret or become aware of something through the senses (sight, hearing, taste, smell or touch)	0	0	0	0
CHEC40 - Lack of significant job aids	0	0	0	0
CHEC41 - Distraction /Task Interruption	0	0	0	0
CHEC42 - Time-of-Day	0	0	0	0

organisations felt the IS-CHEC technique was applicable to an information security setting. This included that no further changes were required to the technique and that the study and use of the IS-CHEC technique had introduced positive benefits including a greater understanding of their incidents, plus the proportions of human error and underlying causes. Other themes included acceptance and acknowledgment that people will make mistakes, they should move away from a blame culture as people are actually well intentioned and want to do a good job and that the organisation should take responsibility for failings. The most prominent themes related to organisational maturity at the beginning of the study, but more importantly how essential organisational buy-in was in order to achieve success.

All seven interviewees explicitly stated that the tool was applicable to an information security implementation. The private sector organisation COO stated: ''It works for us. I don't know whether that's because of the type of things we're doing in terms of the amount of paper and physical manual processing. I think it definitely works for us''. A theme in the responses was also that the technique provided a simple mechanism to understand the specific details of the incident through the GISAT component and the root cause analysis and that it was applicable to a service provider situation with close working relationship with clients. The private sector organisation ISM stated: ''It is a fundamental way of our business working well. Especially, with the nature of our clients and what they want to see''. In addition, interestingly, it was suggested that the technique should be expanded for all types of incidents and not be restricted to the management of information security incidents only, due to the common element being people and the successful results obtained.

The responses from all seven of the interviewees provided views that they felt no changes were required to the IS-CHEC technique, as it has proved to be simple, understandable and effective. The public sector organisation HoS&IA stated: ''I don't think the IS-CHEC technique needs to be amended. I think the way it is currently works'' and the private sector organisation Information Security Incident Analyst stated: ''There are no improvements needed.

The private sector organisation expressed a key tangible benefit of the study and adoption of the IS-CHEC technique was the reduction in information security incidents and the fact that tolerances of human error could be documented and demonstrated to clients with their SIRO stating: ''. . . measurable benefits of a massive reduction in our information security incidents'' and ''It's adding credibility to the information. It's always about backing up any answers that we give with data and it gives us that data to be able to say this happened and this is what we did because of this. To go to client sessions and be able to evidence off the back of this is massively powerful''. The private sector organisation ISM also stated ''. . . seeing the incident numbers come down from where we were which improves our client relationship''. The public sector organisation did not experience a reduction in incident volumes, in fact they increased over the course of the study, but felt that they would make improvements now that they were in a more mature and informed position from the Board-level down. The public sector HoS&IA stated: ''. . . one of the most positive effects is Board awareness of security incidents, where I think a year and a half ago we only really got annual figures. Mainly, because the data wasn't there'' and the Deputy SIRO also stated: ''The positive effect is we understand a lot better where our root causes are

TABLE 6. Private sector CHECs.

CHEC	Most Significant	Second Most Significant	Least Significant	Total
CHEC17 - Little or no independent checking or testing of output	70	29	8	107
CHEC7 - No obvious means of reversing an unintended action	14	62	1	77
CHEC2 - A shortage of time available for error detection and correction	61	8	0	69
CHEC34 - Prolonged inactivity or highly repetitious low mental workload tasks	2	0	52	54
CHEC39 - Little or no self-checking or testing of output	42	4	3	49
CHEC15 - Inexperience of the person performing the task	29	10	0	39
CHEC11 - The person performing the task does not fully understand the policy, standards, process or procedures they are required to adhere to	16	8	8	32
CHEC16 - Inaccurate or incomplete information communicated by procedures, or from a person to a person	21	10	0	31
CHEC1 - Unfamiliarity with a task or situation which is potentially important but which only occurs infrequently or which is novel	10	5	0	15
CHEC6 - A mismatch between an operator's model of the world and that imagined by a designer	11	2	1	14
CHEC9 - Person performing the task required to learn a new technique, process, procedure or way of working which differs in attitude or way of thinking to the previous one	6	8	0	14
CHEC36 - Pressure from someone else to increase the speed or pace at which a task is performed, beyond an individual's preferred pace and capability	9	4	1	14
CHEC32 - Information displayed and how this is applied within procedures or working practices is not fully understood	11	1	1	13
CHEC4 - Too easy to switch off, disable or incorrectly modify alerts, notifications, messages, or inputs leading to important information being missed or not acted upon	3	8	1	12
CHEC19 - Not enough information to allow completeness or accuracy checks to be undertaken	2	2	0	4
CHEC29 - High-level emotional stress	4	0	0	4
CHEC8 - Person performing the task is monitoring numerous incoming information channels at the same time, such as numerous computer monitors	2	0	1	3
CHEC12 - The person performing the task does not understand the actual risk exposure	3	0	0	3
CHEC13 - The system information communicated is inaccurate, unclear or inappropriate	3	0	0	3
CHEC26 - No obvious way to keep track of progress during an activity	0	0	3	3
CHEC3 - Too many alerts, notifications, messages or inputs leading to important information not being seen or heard and acted upon	0	1	1	2
CHEC22 - Little opportunity, such as rest breaks, to exercise mind and body outside the immediate confines of a job	1	0	0	1
CHEC24 - A need for decision making which is beyond the capabilities or experience of the person performing the task	1	0	0	1
CHEC25 - Unclear allocation of role and responsibility	1	0	0	1
CHEC28 - Person performing the task is unaware of its significance and their contribution to corporate objectives	0	1	0	1
CHEC30 - Evidence of ill-health amongst operatives, especially fever	0	1	0	1
CHEC5 - No means of communicating information in a form which can be understood and used	0	0	0	0
CHEC10 - The need to transfer specific knowledge from task to task without loss	0	0	0	0
CHEC14 - The system information which confirms that an action has been successfully completed is delayed, takes too long or does not happen	0	0	0	0
CHEC18 - A conflict between immediate and long-term objectives	0	0	0	0
CHEC20 - A mismatch between the educational achievement level of an individual and the requirements of the task	0	0	0	0
CHEC21 - An incentive to use other more dangerous procedures	0	0	0	0

TABLE 6. *(Continued.)* **Private sector CHECs.**

CHEC	Most Significant	Second Most Significant	Least Significant	Total
CHEC23 - Unreliable instrumentation used to communicate information leading to lack of trust and person performing the task ignoring information	0	0	0	0
CHEC27 - Task requirement exceeds the physical capabilities of the person performing the task	0	0	0	0
CHEC31 - Low workforce morale	0	0	0	0
CHEC33 - A poor or hostile environment (below 75% of health or life-threatening severity)	0	0	0	0
CHEC35 - Disruption of normal work-sleep cycles	0	0	0	0
CHEC37 - Additional team members over and above those necessary to perform task normally and satisfactorily	0	0	0	0
CHEC38 - Age of personnel performing perceptual tasks requiring the ability to interpret or become aware of something through the senses (sight, hearing, taste, smell or touch)	0	0	0	0
CHEC40 - Lack of significant job aids	0	0	0	0
CHEC41 - Distraction /Task Interruption	0	0	0	0
CHEC42 – Time-of-Day	0	0	0	0

related to staff error than we ever did before''. In terms of senior management education, the private sector organisation COO stated: ''I haven't done this type of technique. I think, it has helped educate me around the level of expectation and the level of risk that's introduced with lots of human handling around things and to help take that step back and look at what we need to do and what we need to focus on. So, I've definitely learned that, because, if this wasn't done I think we would still be scratching our head around some of this''.

As a result of the study, all seven interviewees demonstrated a good awareness of incidents, the proportions and effects of human error on the organisation. As expected, the senior managers in both organisations were not aware of the specific IS-CHEC technique component names but were able to express an accurate understanding of human error in terms of holistic views relating to trends, reporting and underlying causes as a result of using the IS-CHEC technique. The public sector HoS&IA demonstrated a confirmed understanding when a response to one of the questions stated: ''...we had an understanding, an idea, that most of our incidents were to do with human error, but we didn't really have the stats and management information to back that up''. Whereas the private sector organisation ISM was surprised by the confirmed proportions of human error in one of their responses: ''I was not aware of the high numbers of human error before this work, and it is quite alarming. It is not unsurprising now that we have seen the data, because it is so easy to make a simple mistake''. Responses also showed a greater understanding of staff culture within respective organisations.

As a result of the enhanced organisational understanding in both organisations, there was an acceptance and acknowledgment that people will make mistakes and a need to move away from a blame culture. As an example of this, the private sector COO stated: ''...let's face facts, people will always make mistakes. So, there will always be an element of human error if you've got highly manual processing. So we should accept that that does happen''. To support this view the public sector organisation interviewees provided a form of empathy with employees of the organisation in that they should not be perceived as intentionally wanting to negatively impact the organisation with the ISM stating: ''What I've learned is that people generally want to do a good job. An effective job, in a secure way. They don't want to be sending individuals' personal data to the wrong people. The closer understanding of the people that error pertained to showed a desire to operate good security practices with the HoS&IA also stating: ''I think before we engaged in this, I don't think we believed that staff were really security minded, but, I think, it has opened my eyes that they are. Obviously, not all staff are, but a lot more than what I gave credit for''.

With a greater understanding of responsibility that rests with the organisation rather than the individual that has suffered an error whilst performing their role, both organisations also conveyed that they were conscious that there was a responsibility of the organisation to provide an environment for their people that reduced the potential for human error. The public sector organisation Deputy SIRO stated: ''...I want to fully understand why that mistake happened, where did the process let the human being down and what can we do to help a human being not do that again and this technique just gives us all that'' which was a view that was reinforced by the same organisation's ISM who said the following: ''...let's put the right controls in place to make sure it doesn't happen again, rather than attack the individual who's probably actually been a victim of whatever the cause is. And it's really helped in that way''.

TABLE 7. Public & Private sector RPMs.

Public Sector RPM	Effectiveness	Total	Private Sector RPM	Effectiveness	Total
RPM1 – Awareness and training undertaken (including 1:1)	Lower	112	RPM1 – Awareness and training undertaken (including 1:1)	Lower	268
RPM6 – Increased supervision or checks	Moderate	84	RPM5 – Change to, simplification or standardisation of existing procedures, tools, systems or practices	Higher	114
RPM5 – Change to, simplification or standardisation of existing procedures, tools, systems or practices	Higher	21	RPM6 – Increased supervision or checks	Moderate	113
RPM0 – None needed	N/A	18	RPM2 – Procedures documented and communicated	Lower	38
RPM2 – Procedures documented and communicated	Lower	7	RPM19 – Recover, collect or destroy information or equipment	Lower	34
RPM8 – Risk assessment or audit undertaken and acted upon	Moderate	5	RPM20 – Reissue or resend information or equipment	Lower	28
RPM99 – Other non-human error related remedial and preventative measure	N/A	5	RPM0 – None needed	N/A	14
RPM13 – Acquire and introduce new tools or technology	Higher	1	RPM4 – Recruitment of additional staff	Moderate	10
RPM3 – Simulation exercises performed	Moderate	1	RPM99 – Other non-human error related remedial and preventative measure	N/A	9
RPM10 – Change to work patterns such as frequent breaks	Moderate	0	RPM8 – Risk assessment or audit undertaken and acted upon	Moderate	6
RPM11 – Job rotation	Moderate	0	RPM7 – Change to communication methods	Moderate	4
RPM12 – Incentives introduced	Lower	0	RPM13 – Acquire and introduce new tools or technology	Higher	3
RPM14 – Introduce robotics/automation/artificial intelligence	Higher	0	RPM14 – Introduce robotics/automation/artificial intelligence	Higher	3
RPM15 – Split process and introduce segregation of duties	Moderate	0	RPM3 – Simulation exercises performed	Moderate	1
RPM16 – Eliminate or reduce distractions	Moderate	0	RPM9 – Job description checked and updated	Lower	0
RPM17 – Eliminate look-and-sound-alikes	Moderate	0	RPM10 – Change to work patterns such as frequent breaks	Moderate	0
RPM18 – Introduce warnings, alerts or alarms	Lower	0	RPM11 – Job rotation	Moderate	0
RPM19 – Recover, collect or destroy information or equipment	Lower	0	RPM12 – Incentives introduced	Lower	0
RPM20 – Reissue or resend information or equipment	Lower	0	RPM15 – Split process and introduce segregation of duties	Moderate	0
RPM4 – Recruitment of additional staff	Moderate	0	RPM16 – Eliminate or reduce distractions	Moderate	0
RPM7 – Change to communication methods	Moderate	0	RPM17 – Eliminate look-and-sound-alikes	Moderate	0
RPM9 – Job description checked and updated	Lower	0	RPM18 – Introduce warnings, alerts or alarms	Lower	0

There were a couple of core themes relating to challenges that were raised in the interviews pertaining to initial organisational maturity and buy-in. With regard to initial maturity the public sector organisation stated: ''…this was not just a step to the next level, but a step up a number of levels to what we were doing'' and also relating to the position at the end of the study ''…this has taken us to the next level. I think, all the reports and MI we are getting, the KPIs we are building from our side now put us on a good foot''. This shows that the organisation has, despite initial challenges, demonstrated significant progress in terms of incident management maturity through the study and use of the IS-CHEC technique. The private sector organisation was felt to already be in a mature position with regard to information security incident management although the ISM did state: ''...we would need good reporting from the outset'' showing that improvements were needed to realise improvements quicker than experienced throughout the study.

The most significant challenge for both organisations related to initial buy-in from the wider organisation and sub-contractors to adopt a new way of working and the integration of the IS-CHEC technique. Also, making the technique understandable, and simple, to all people that needed to interact with it as part of the incident management function. However, both organisations clearly presented that through education, greater understanding and demonstrating the benefits to the organisation, specific business areas and individuals, the resistance was reduced and full engagement and buy-in obtained over the course of the study. As examples of this, the private sector organisation SIRO stated: ''Working with third parties is never easy and third parties when you're subcontracting to them…there's scepticism initially, but they have seen the benefits of it. Not just our customers also our subcontractors have certain benefits and it's delivered for their organisation. I think both a challenge and an achievement in that respect'', and the public sector

TABLE 8. Semi-structured interview response codes.

Code	Participating Organisation	Question 1: Understanding & Impact	Question 2: Applicability	Question 3: Positive Effects	Question 4: Challenges	Question 5: New Learning	Question 6: Suggested Changes	Question 7: Opinions & Feelings	Total Count
Acceptance of human error	Private Sector	4	0	0	0	1	0	0	5
	Public Sector	1	1	0	0	2	0	1	5
Buy-In	Private Sector	1	1	5	14	3	4	0	28
	Public Sector	1	0	7	7	2	4	0	21
Expand for all types of incidents	Private Sector	0	2	0	0	0	0	2	4
	Public Sector	0	0	0	0	0	0	0	0
Improved client relationship	Private Sector	1	0	3	0	0	0	1	5
	Public Sector	0	0	0	0	0	0	0	0
Incident understanding	Private Sector	9	3	5	9	9	3	1	39
	Public Sector	16	6	9	1	7	1	3	43
IS-CHEC components understanding	Private Sector	9	2	1	2	1	0	0	15
	Public Sector	1	2	2	0	0	3	0	8
No change required to the technique	Private Sector	0	0	0	0	0	3	3	6
	Public Sector	0	0	0	0	0	5	2	7
Proactive use for quality management	Private Sector	0	1	0	0	0	0	1	2
	Public Sector	0	0	0	0	0	0	0	0
Reduction in incident volumes	Private Sector	2	2	3	1	0	0	1	9
	Public Sector	0	0	1	0	2	0	1	4
Remedial and preventative measures	Private Sector	6	2	1	4	3	0	0	16
	Public Sector	1	3	1	0	1	1	0	7
Reporting	Private Sector	2	2	2	4	4	4	1	19
	Public Sector	3	2	4	0	0	4	3	16
Risk understanding	Private Sector	2	0	0	0	1	0	0	3
	Public Sector	3	2	1	0	0	0	0	6
Simple uncomplicated tool	Private Sector	2	3	4	8	0	1	1	19
	Public Sector	0	0	2	0	0	0	0	2
Tolerances and expectations	Private Sector	3	0	1	0	1	0	0	5
	Public Sector	2	2	0	0	1	1	0	6
Trend analysis	Private Sector	4	1	0	0	3	0	0	8
	Public Sector	6	1	2	0	0	0	1	10
Valuable, productive and beneficial	Private Sector	3	2	2	3	0	0	0	10
	Public Sector	6	4	8	2	0	1	8	29
Works well and applicable	Private Sector	1	8	4	1	2	1	2	19
	Public Sector	3	7	5	1	0	2	8	26

organisation HoS&IA stated: "…its been difficult in some areas to get across to the staff the importance of why we are doing this…once you sit down and you talk through the benefits and start sharing the MI and analysis that we're getting, then they do understand it".

Comparison: The organisations expressed very similar patterns in terms of improved information security incident management maturity and challenges around wider organisational buy-in. The key theme across both organisations was an increased understanding of their respective employees, their behaviours and challenges and context they work in, which can affect information security posture.

VI. DISCUSSION

A. PRINCIPAL FINDINGS

The principal finding of the research was providing further evidence that the vast majority of information security incidents do indeed pertain to human error, which supports our previous work [8], [9], [45]. In the case of both organisations, the mean average of proportions reported human error related

TABLE 9. Semi-Structured Interview Response Word Frequency.

Private Sector Organisation			Public Sector Organisation		
Word	Count	Weighted Percentage (%)	Word	Count	Weighted Percentage (%)
think	270	3.67	think	288	3.93
incidents	111	1.51	know	125	1.71
actually	99	1.35	incidents	117	1.60
people	95	1.29	helped	85	1.16
know	94	1.28	security	81	1.11
works	78	1.06	process	80	1.09
need	71	0.97	actually	78	1.07
helped	68	0.93	people	76	1.04
process	64	0.87	need	76	1.04
looking	62	0.84	cause	64	0.87
information	52	0.71	technique	62	0.85
technique	49	0.67	error	58	0.79
time	49	0.67	works	57	0.78
understand	49	0.67	terms	55	0.75
business	48	0.65	understand	53	0.72
security	48	0.65	months	50	0.68
error	47	0.64	staff	49	0.67
cause	47	0.64	happening	49	0.67
CHECs	46	0.63	business	45	0.61
something	45	0.61	data	44	0.60

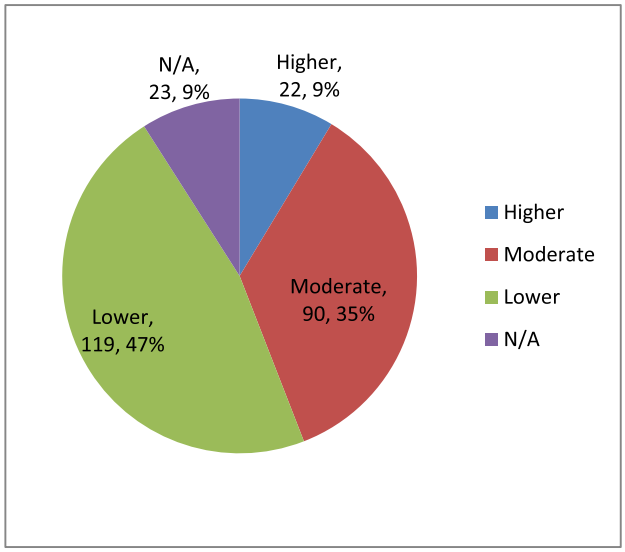


FIGURE 4. Public sector RPM effectiveness percentages.

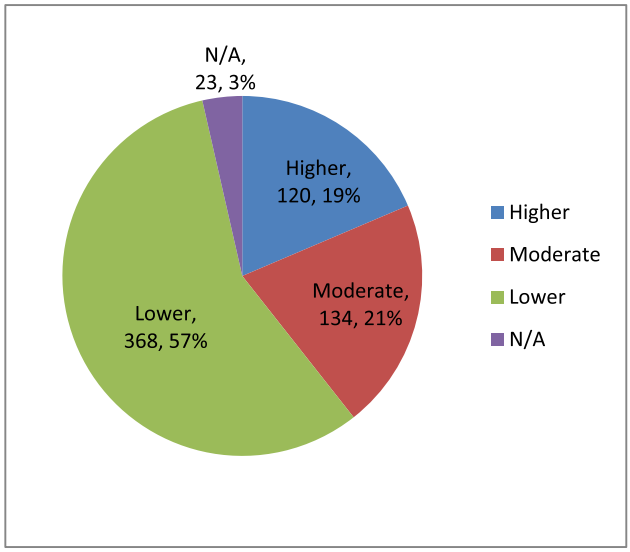


FIGURE 5. Private sector RPM effectiveness percentages.

information security incidents over the 12 month period was 79% for the public sector organisation and 89% for the private sector of all reported incidents.

A key finding from the independent case study research undertaken in both organisations showed that the volumes of information security incidents and human error and trend differed for both organisations. The public sector organisation incidents fluctuated, but had a general increase up to month 10 and subsequent decrease in months 11 and 12. The public sector was actively building maturity in terms of information security understanding through recruitment of dedicated personnel, changes to systems and communication campaigns

TABLE 10. Incident volumes.

	Status	Count		
		Month 1	Month 2	Month 3
Information security incidents	↓			
Human error related information security incidents	↑			
Incidents where Root Cause Analysis has not yet been completed within agreed 5 days duration	↔			
Incidents under investigation and remain in tolerance of the 5 days SLA	↓			
% Human error where root cause is known	↑			

TABLE 11. Human Error Information Security Incidents by Business Area.

Business Area	Status	Count		
		Month 1	**Month 2**	**Month 3**
Area 1	↓			
Area 2	↑			
Area 3	↔			

TABLE 12. RPMS by Month.

RPM	Count		
	Month 1	Month 2	Month 3
Most Common RPM (Effectiveness)			
…			
Least Common RPM (Effectiveness)			

TABLE 13. RPMs by Business Area.

RPM	Count		
	Area 1	Area 2	Area 3
Most Common RPM (Effectiveness)			
…			
Least Common RPM (Effectiveness)			

TABLE 14. All RPMs.

RPM	Count	Title/ Description	Owner	Deadline	Status
RPM 1					
RPM 2					

TABLE 15. GISAT by Business Area.

GISAT	Count		
	Area 1	Area 2	Area 3
Most Common GISAT			
…			
Least Common GISAT			

across the organisation. This is evident in month 1, where 4 incidents were reported and recorded, which was not reflective of the actual organisational position. The adoption of the IS-CHEC technique allowed the public sector organisation to focus on capturing incidents and their underlying causes and is now in a much stronger and informed position. The private sector organisation, however, was in a more established and mature position in terms of personnel, systems and organisational understanding at the start of the 12 month study. They benefitted from a general trend of decreasing incident volumes over the study period, as well as bettering their understanding on the causes of human error, which continued to account for the majority of incident root causes.

The study, through the use of Pearson's Correlation Coefficient, also established that within both organisations there was a strong linear relationship between the total numbers of recorded information security incidents and the proportions of human error related incidents.

The qualitative data captured as part of the semi-structured interviews supports the primary motivation behind the study, which was to enable greater understanding of the proportions of human error related information security incidents and their underlying causes. According to all interview participants, the IS-CHEC technique added benefits for their role

TABLE 16. GISAT by Month.

GISAT	Status	Count		
		Month 1	**Month 2**	**Month 3**
Most Common GISAT				
…				
Least Common GISAT				

TABLE 17. Count of Systems or Processes & Nominal Likelihood of Failure.

<Lower Bound	**<= Nominal Likelihood AND > Lower Bound**	**>= Nominal Likelihood AND < Upper Bound**	**> Upper Bound**

TABLE 18. Most Common Systems or Processes & HEART Nominal Likelihood of Failure & Actual Likelihood of Failure.

Business Area	System or Process	GISAT	GISAT Count p/a	Count of Incidents	HEART Likelihood of Failure	HEART Lower Bound	HEART Upper Bound	Actual Likelihood of Failure

TABLE 19. Systems or Processes by Business Area.

System or Process	Count		
	Area 1	Area 2	Area 3
Most Common System or Process			
…			
Least Common System or Process			

TABLE 20. Most Significant CHECs.

CHEC	Count		
	Area 1	Area 2	Area 3
Most Common CHEC			
…			
Least Common CHEC			

**Also same table format for second most significant and least significant CHECs*

TABLE 21. Total CHECs.

CHEC	Status	Count		
		Month 1	**Month 2**	**Month 3**
Most Common CHEC				
…				
Least Common CHEC				

and respective organisation and was applicable to an information security setting, although success is dependent upon effective organisational buy-in.

The study provides further evidence that HRA can be used to support retrospective and predictive analysis of information security [38]. The study also reinforced and demonstrated views expressed in that the main cause of information security incidents relates to an organisation's employees [29]. The case study also presents data supporting an argument against the low proportions of human factor root causes of incidents and breaches presented in literature [26], [50].

B. IMPLICATIONS OF THE FINDINGS

The research provides solid evidence that the information security field would benefit from the formal development and application of HRA techniques, such as IS-CHEC, to address the issue of human error and its information security impact which is not currently the case. HRA is established within the safety field, and the information security field would benefit from these methods too as a common denominator is the people that are an integral component of both.

C. LIMITATIONS OF THE METHOD

The research found that the time taken to undertake the root cause analysis within both organisations took longer than

TABLE 22. Mapping of CHECs to RPMs.

CHEC	RPM
CHEC1 - Unfamiliarity with a task or situation which is potentially important but which only occurs infrequently or which is novel	RPM1 - Awareness and training undertaken
	RPM2 - Procedures documented and communicated
	RPM3 - Simulation exercises performed
	RPM6 - Increased supervision or checks
	RPM14 – Introduce robotics/automation/artificial intelligence
	RPM18 – Introduce warnings, alerts or alarms
CHEC2 - A shortage of time available for error detection and correction	RPM4 - Recruitment of additional staff
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 - Increased supervision or checks
	RPM14 – Introduce robotics/automation/artificial intelligence
	RPM17 – Eliminate look-and-sound-alikes
	RPM18 – Introduce warnings, alerts or alarms
CHEC3 - Too many alerts, notifications, messages or inputs leading to important information not being seen or heard and acted upon	RPM4 - Recruitment of additional staff
	RPM5 - Change to existing procedures, tools or practices
	RPM7 – Change to communication methods
	RPM14 – Introduce robotics/automation/artificial intelligence
	RPM16 – Eliminate or reduce distractions
	RPM17 – Eliminate look-and-sound-alikes
	RPM18 – Introduce warnings, alerts or alarms
CHEC4 - Too easy to switch off, disable or incorrectly modify alerts, notifications, messages or inputs leading to important information being missed or not acted upon	RPM1 – Awareness and training undertaken (including 1:1)
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 - Increased supervision or checks
	RPM13 – Access control changes applied
CHEC5 - No means of communicating information in a form which can be understood and used	RPM2 - Procedures documented and communicated
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM7 - Change to communication methods
CHEC6 - A mismatch between an operator's model of the world and that imagined by a designer	RPM1 - Awareness and training undertaken

TABLE 22. *(Continued.)* **Mapping of CHECs to RPMs.**

CHEC	RPM
	RPM5 - Change to existing procedures, tools, systems or practices
CHEC7 - No obvious means of reversing an unintended action	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 – Increased supervision or checks
	RPM18 – Introduce warnings, alerts or alarms
CHEC8 - Person performing the task is monitoring numerous incoming information channels at the same time, such as numerous computer monitors	RPM2 - Procedures documented and communicated
	RPM4 – Recruitment of additional staff
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM7 - Change to communication methods
	RPM14 – Introduce robotics/automation/artificial intelligence
	RPM17 – Eliminate look-and-sound-alikes
	RPM18 – Introduce warnings, alerts or alarms
CHEC9 - Person performing the task required to learn a new technique, process, procedure or way of working which differs in attitude or way of thinking to the previous one	RPM1 - Awareness and training undertaken
	RPM5 – Change to existing procedures, tools, systems or practices
CHEC10 - The need to transfer specific knowledge from task to task without loss	RPM1 - Awareness and training undertaken
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM14 – Introduce robotics/automation/artificial intelligence
CHEC11 - The person performing the task does not fully understand the policy, standards, process or procedures they are required to adhere to	RPM1 - Awareness and training undertaken
	RPM2 - Procedures documented and communicated
	RPM5 - Change to existing procedures, tools, systems or practices
CHEC12 - The person performing the task does not understand the actual risk exposure	RPM1 - Awareness and training undertaken
	RPM8 - Risk assessment undertaken and acted upon
CHEC13 - The system information communicated is inaccurate, unclear or inappropriate	RPM5 - Change to existing procedures, tools, systems or practices
	RPM7 – Change to communication methods
	RPM17 – Eliminate look-and-sound-alikes
	RPM18 – Introduce warnings, alerts or alarms
CHEC14 - The system information which confirms that an action has been successfully completed, is delayed, takes too long or does not happen	RPM5 - Change to existing procedures, tools, systems or practices
	RPM7 – Change to communication methods
CHEC15 - Inexperience of the person performing the task	RPM1 - Awareness and training undertaken
	RPM4 – Recruitment of additional staff
	RPM6 - Increased supervision or checks
	RPM18 – Introduce warnings, alerts or alarms
CHEC16 - Inaccurate or incomplete information communicated by	RPM1 – Awareness and training undertaken (including 1:1)

TABLE 22. *(Continued.)* **Mapping of CHECs to RPMs.**

CHEC	RPM
procedures, or from a person to a person	RPM2 - Procedures documented and communicated
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM7 - Change to communication methods
	RPM16 – Eliminate or reduce distractions
CHEC17 - Little or no independent checking or testing of output	RPM4 - Recruitment of additional staff
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 - Increased supervision or checks
	RPM14 – Introduce robotics/automation/artificial intelligence
	RPM15 – Split process and introduce segregation of duties
	RPM18 – Introduce warnings, alerts or alarms
CHEC18 - A conflict between immediate and long-term objectives	RPM1 - Awareness and training undertaken
	RPM6 - Increased supervision or checks
	RPM8 – Risk assessment undertaken and acted upon
CHEC19 - Not enough information to allow completeness or accuracy checks to be undertaken	RPM5 - Change to existing procedures, tools, systems or practices
	RPM7 - Change to communication methods
CHEC20 - A mismatch between the educational achievement level of an individual and the requirements of the task	RPM1 - Awareness and training undertaken
	RPM4 – Recruitment of additional staff
	RPM9 - Job description checked and updated
CHEC21 - An incentive to use other more dangerous procedures	RPM1 - Awareness and training undertaken
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 – Increased supervision or checks
CHEC22 - Little opportunity, such as rest breaks, to exercise mind and body outside the immediate confines of a job	RPM1 - Awareness and training undertaken
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM10 - Change to work patterns such as frequent breaks
	RPM11 – Job rotation
CHEC23 - Unreliable instrumentation used to communicate information leading to lack of trust and person performing the task ignoring information	RPM5 - Change to existing procedures, tools, systems or practices
	RPM7 – Change to communication methods
	RPM18 – Introduce warnings, alerts or alarms
CHEC24 - A need for decision making which is beyond the capabilities	RPM1 - Awareness and training undertaken

TABLE 22. *(Continued.)* **Mapping of CHECs to RPMs.**

CHEC	RPM
or experience of the person performing the task	RPM4 – Recruitment of additional staff
	RPM6 - Increased supervision or checks
	RPM18 – Introduce warnings, alerts or alarms
CHEC25 - Unclear allocation of role and responsibility	RPM1 - Awareness and training undertaken
	RPM9 - Job description checked and updated
CHEC26 - No obvious way to keep track of progress during an activity	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 – Increased supervision or checks
CHEC27 - Task requirement exceeds the physical capabilities of the person performing the task	RPM4 – Recruitment of additional staff
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM8 - Risk assessment undertaken and acted upon
CHEC28 - Person performing the task is unaware of its significance and their contribution to corporate objectives	RPM1 - Awareness and training undertaken
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM9 - Job description checked and updated
	RPM11 - Job rotation
CHEC29 - High-level emotional stress	RPM1 - Awareness and training undertaken
	RPM4 - Recruitment of additional staff
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 - Increased supervision or checks
	RPM16 – Eliminate or reduce distractions
CHEC30 - Evidence of ill-health amongst operatives, especially fever	RPM1 - Awareness and training undertaken
	RPM6 - Increased supervision or checks
CHEC31 - Low workforce morale	RPM1 - Awareness and training undertaken
	RPM4 - Recruitment of additional staff
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 - Increased supervision or checks
	RPM9 - Job description checked and updated
	RPM12 - Incentives introduced
CHEC32 - Information displayed and how this is applied within procedures or working practices is not fully understood	RPM1 - Awareness and training undertaken
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM7 – Change to communication methods

TABLE 22. *(Continued.)* **Mapping of CHECs to RPMs.**

CHEC	RPM
	RPM17 – Eliminate look-and-sound-alikes
	RPM18 – Introduce warnings, alerts or alarms
CHEC33 - A poor or hostile environment (below 75% of health or life-threatening severity)	RPM1 - Awareness and training undertaken
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 - Increased supervision or checks
CHEC 34 - Prolonged inactivity or highly repetitious low mental workload tasks	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 - Increased supervision or checks
	RPM11 - Job rotation
	RPM14 – Introduce robotics/automation/artificial intelligence
	RPM16 – Eliminate or reduce distractions
	RPM17 – Eliminate look-and-sound-alikes
	RPM18 – Introduce warnings, alerts or alarms
CHEC 35 - Disruption of normal work-sleep cycles	RPM4 - Recruitment of additional staff
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 - Increased supervision or checks
CHEC 36 - Pressure from someone else to increase the speed or pace at which a task is performed, beyond an individual's preferred pace and capability	RPM1 – Awareness and training undertaken (including 1:1)
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 - Increased supervision or checks
	RPM17 – Eliminate look-and-sound-alikes
	RPM18 – Introduce warnings, alerts or alarms
CHEC 37 - Additional team members over and above those necessary to perform task normally and satisfactorily	RPM5 - Change to existing procedures, tools, systems or practices
CHEC 38 - Age of personnel performing perceptual tasks requiring the ability to interpret or become aware of something through the senses (sight, hearing, taste, smell or touch)	RPM4 – Recruitment of additional staff
	RPM6 - Increased supervision or checks
	RPM17 – Eliminate look-and-sound-alikes
	RPM18 – Introduce warnings, alerts or alarms
CHEC 39 - Little or no self-checking or testing of output	RPM4 - Recruitment of additional staff
	RPM5 - Change to existing procedures, tools, systems or practices
	RPM6 - Increased supervision or checks
	RPM15 – Split process and introduce segregation of duties
	RPM18 – Introduce warnings, alerts or alarms
CHEC40 - Lack of significant job aids	RPM5 – Change to existing procedures, tools, systems or practices

TABLE 22. *(Continued.)* **Mapping of CHECs to RPMs.**

CHEC	RPM
	RPM13 – Acquire and introduce new tools or technology
CHEC41 - Distraction /Task Interruption	RPM6 - Increased supervision or checks
	RPM13 – Acquire and introduce new tools or technology
	RPM16 – Eliminate or reduce distractions
	RPM18 – Introduce warnings, alerts or alarms
CHEC42 – Time-of-Day	RPM4 – Recruitment of additional staff
	RPM6 – Increased supervision or checks
	RPM10 – Change to work patterns such as frequent breaks
	RPM11 – Job rotation
	RPM18 – Introduce warnings, alerts or alarms

TABLE 23. **Public Sector Organisation Correlation Data.**

Month	Total Incidents (x)	$x - \bar{x}$	$(x - \bar{x})^2$	Total Human Error Incidents (y)	$y - \bar{y}$	$(y - \bar{y})^2$	$(x - \bar{x})(y - \bar{y})$
1	4	-17.1666667	294.6944444	4	-12.6666667	160.444444	217.4444444
2	20	-1.16666667	1.361111111	12	-4.66666667	21.7777778	5.444444444
3	10	-11.1666667	124.6944444	6	-10.6666667	113.777778	119.1111111
4	24	2.83333333	8.027777778	19	2.333333333	5.44444444	6.611111111
5	15	-6.16666667	38.02777778	12	-4.66666667	21.7777778	28.77777778
6	22	0.83333333	0.694444444	15	-1.66666667	2.77777778	-1.38888889
7	31	9.83333333	96.69444444	27	10.33333333	106.777778	101.6111111
8	23	1.83333333	3.361111111	18	1.333333333	1.77777778	2.444444444
9	16	-5.16666667	26.69444444	11	-5.66666667	32.1111111	29.27777778
10	31	9.83333333	96.69444444	27	10.33333333	106.777778	101.6111111
11	30	8.83333333	78.02777778	25	8.333333333	69.4444444	73.61111111
12	28	6.83333333	46.69444444	24	7.333333333	53.7777778	50.11111111
Total	254	0	815.6666667	200	0	696.666667	734.6666667

$\bar{x} = 21.16667$; $\bar{y} = 16.66667$; $r = 0.974589$

expected with an average of 37% public sector incidents having their expected root cause analysis completed within the 5-day expectation and 71.5% for the private sector organisation. Also public sector reported incidents on average were open for 49.3 working days before they were closed and the private sector organisation for 40.5 working days. This impacted upon the speed of selection and implementation of RPMs, but also resulted in the monthly IS-CHEC reports containing incomplete information, which were required to enable strategic action to be taken. It was also found that the time duration from incident reporting to incident closure did not happen quickly, which again added delay to experiencing the intended organisational benefits, such as a reduction in incident volumes.

A limitation of the method is also that it is dependent on a mature and established information security culture, whereby all employees are aware of what constitutes an information security incident and that they must all be reported. Both organisations acted independently in the recruitment of additional personnel to process information security incidents during the research as a result of the continuous analysis of incident volumes and trends. As HRA was not established within information security practices prior to the research, there was a continual state of learning for all involved, which

TABLE 24. Private Sector Organisation Correlation Data.

Month	Total Incidents (x)	$x - \bar{x}$	$(x - \bar{x})^2$	Total Human Error Incidents (y)	$y - \bar{y}$	$(y - \bar{y})^2$	$(x - \bar{x})(y - \bar{y})$
1	45	15	225	44	17.16666667	294.6944444	257.5
2	38	8	64	32	5.166666667	26.69444444	41.33333333
3	30	0	0	29	2.166666667	4.694444444	0
4	39	9	81	33	6.166666667	38.02777778	55.5
5	52	22	484	49	22.16666667	491.3611111	487.6666667
6	23	-7	49	21	-5.833333333	34.02777778	40.83333333
7	23	-7	49	19	-7.833333333	61.36111111	54.83333333
8	27	-3	9	24	-2.833333333	8.027777778	8.5
9	8	-22	484	8	-18.83333333	354.6944444	414.3333333
10	23	-7	49	19	-7.833333333	61.36111111	54.83333333
11	28	-2	4	27	0.166666667	0.027777778	-0.33333333
12	24	-6	36	17	-9.833333333	96.69444444	59
Total	360	0	1534	322	0	1471.666667	1474

$\bar{x} = 30$; $\bar{y} = 26.83333$; $r = 0.981025$

also included newly recruited information security personnel. In addition, the public sector organisation in particular struggled to obtain buy-in and collaboration from the wider business areas to enable incidents to be processed as quickly as desired.

As this research was applied to two independent public and private sector organisations, the findings are felt to be generally applicable to organisations outside of this research that undertake large amounts of manual processing of personal or confidential information. This is due to the common element being people and their behaviour, which is at the core of all organisations. However, as both participating organisations provide healthcare services, there is a potential limitation of the research in that the captured results could present a bias towards the healthcare sector and associated services.

VII. CONCLUSION AND FUTURE WORK

The research found that within the participating organisations the common tasks that were being performed and associated with incidents were administrative tasks, which related to the communication, editing or storage of confidential or personal information. The research also established that the most common cause of human error related information security incidents was a lack of checking to detect and protect against human fallibility. It was also notable that in both organisations the most common RPM was RPM1 – Awareness and training undertaken (including 1:1), which has a lower effectiveness due to the fact that it relies upon memory to prevent a reoccurrence [49]. It was also noticeable that the private sector organisation was willing to apply more remedial and preventative measures to address human error, and, in particular, difficult measures that attract a higher effectiveness were successful in benefiting from a clear and recognisable reduction in both human error and overall information security incidents.

This research provides empirical evidence and clarity to the information security community as to the high proportions of human error that should be expected and catered for. In addition, it was found that although the volumes of human error related incidents occurring in both participating organisations fluctuated over the 12 month period, the proportions of human error remained consistently as the majority root cause. It was also established that both organisations experienced a strong linear relationship between the total number of incidents and the proportions of human error

related incidents. This provides a view that the IS-CHEC technique was successful in providing benefit through increased understanding of human error risk exposure for the participating organisations and either reduced or reducing incident volumes following a peak, which coincided with organisational awareness and understanding campaigns. However, the fact remains that a common characteristic of a human being is that we will make mistakes and organisations should formally adopt HRA techniques, such as IS-CHEC, to address this fact.

APPENDICES

A. IS-CHEC REPORT TEMPLATE

Introduction
Executive Summary
Human Error Information Security Incidents
Reporting Period

See Tables 10–21.

B. CHEC AND RPM MAPPING

Remedial and preventative measures (RPM) were selected and applied according to the identified Core Human Error Causes (CHEC). A mapping of CHECs and RPMs can be found in Table 22 below to aid selection of consistent and effective controls.

C. PEARSON'S CORRELATION COEFFICIENT DATA

See Tables 23 and 24.

ACKNOWLEDGMENT

The authors thank the editors and the anonymous reviewers for their constructive comments. The funder had no role in study design, data collection and analysis, decision to publish or preparation of the manuscript.

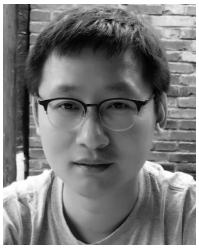
REFERENCES

[1] *Information Security Management Systems—Requirements*, Standard ISO/IEC 27001, BSI, 2013.
[2] *Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS), Version 3.2*, PCI Security Standards Council, Wakefield, MA USA, 2016.
[3] NHS Digital. (2019). *Data Security and Protection Toolkit*. Accessed: Jan. 26, 2019. [Online]. Available: https://www.dsptoolkit.nhs.uk/
[4] D. Gertman, "Part 3: Cyber security and risk assessment?: HRA where art thou?" Tech. Rep., 2013.
[5] C. C. Wood and W. W. Banks, Jr., "Human error: An overlooked but significant information security problem," *Comput. Secur.*, vol. 12, no. 1, pp. 51–60, Feb. 1993.
[6] J. Bell and J. Holroyd, "Review of human reliability assessment methods," *Health Saf. Lab.*, p. 78, 2009.
[7] 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)*, 2018, pp. 911–921.
[8] 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, Jul. 2019.
[9] 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.
[10] J. T. Reason, *Human Error*. Cambridge, U.K.: Cambridge Univ. Press, 1990.
[11] M. Evans, Y. He, C. Luo, I. Yevseyeva, H. Janicke, and L. A. Maglaras, "Employee perspective on information security related human error in healthcare: Proactive use of IS-CHEC in questionnaire form," *IEEE Access*, vol. 7, pp. 102087–102101, 2019.
[12] F. T. Chandler, Y. H. J. Chang, A. Mosleh, J. L. Marble, R. L. Boring, and D. Gertman, "Human reliability analysis methods: Selection guidance for NASA," NASA, Washington, DC, USA, Jul. 2006, p. 175.
[13] L. Johannesen, N. Sarter, and R. Cook, *Behind Human Error*. ProQuest Ebook Central, 2010.
[14] 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.
[15] A. Y. Connolly, M. Lang, J. Gathegi, and D. J. Tygar, "The effect of organisational culture on employee security behaviour: A qualitative study," in *The Effect of Organisational Culture on Employee Security Behaviour: A Qualitative Study*. 2016, pp. 33–44.
[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] A. Alhogail and A. Al Hogail, "Cultivating and assessing an organizational information security culture; An empirical study analyzing human factors and change management principles toward building information security culture view project cultivating and assessing an organizational information security culture; An empirical study," *Artic. Int. J. Secur. Appl.*, vol. 9, no. 7, pp. 163–178, 2015.
[18] 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.
[19] K. Helkala, "Supporting the human in cyber defence," in *Computer Security*. Cham, Switzerland: Springer, 2018, pp. 147–162.
[20] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, "The human factor of information security: Unintentional damage perspective," *Procedia-Social Behav. Sci.*, vol. 147, pp. 424–428, Aug. 2014.
[21] H. Stewart and J. Jürjens, "Information security management and the human aspect in organizations," *Inf. Comput. Secur.*, vol. 25, no. 5, pp. 494–534, Nov. 2017.
[22] R. Alavi, S. Islam, and H. Mouratidis, "An information security risk-driven investment model for analysing human factors," *Inf. Comput. Secur.*, vol. 24, no. 2, pp. 205–227, Jun. 2016.
[23] T. Asai and A. U. Hakizabera, "Human-related problems of information security in East African cross-cultural environments," *Inf. Manage. Comput. Secur.*, vol. 18, no. 5, pp. 328–338, Nov. 2010.
[24] R. Klahr, J. N. Shah, P. Sheriffs, T. Rossington, and G. Pestell, "Cyber security breaches survey 2017: Main report," Tech. Rep., 2017.
[25] 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.
[26] 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.
[27] L. A. Maglaras, G. Drivas, K. Noou, and S. Rallis, "NIS directive: The case of Greece," *ICST Trans. Secur. Saf.*, vol. 4, no. 14, p. e1, 2018.
[28] E. D. Frangopoulos, M. M. Eloff, and L. M. Venter, "Human aspects of information assurance: A questionnaire-based quantitative approach to assessment," in *Proc. HAISA*, 2014, pp. 217–229.
[29] S. Choi, J. T. Martins, and I. Bernik, "Information security: Listening to the perspective of organisational insiders," *J. Inf. Sci.*, vol. 44, no. 6, pp. 752–767, Jan. 2018.
[30] J. Rajamäki, 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.
[31] J. Braband and H. Schäbe, "Probability and security—Pitfalls and chances," *Saf. Rel.*, vol. 36, no. 1, pp. 3–12, Jan. 2016.
[32] *2014 Data Breach Investigations Report*, Verizon Enterprise Solutions, Basking Ridge, NJ, USA, 2014, pp. 1–60.

[33] M. M. Yusof, J. Kuljis, A. Papazafeiropoulou, and L. K. Stergioulas, "An evaluation framework for health information systems: Human, organization and technology-fit factors (HOT-fit)," *Int. J. Med. Inform.*, vol. 77, no. 6, pp. 386–398, Jun. 2008.
[34] 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)," Tech. Rep., 2015.
[35] R. Khajouei, R. Abbasi, and M. Mirzaee, "Errors and causes of communication failures from hospital information systems to electronic health record: A record-review study," *Int. J. Med. Inform.*, vol. 119, pp. 47–53, Nov. 2018.
[36] P. C. Cacciabue and G. Vella, "Human factors engineering in healthcare systems: The problem of human error and accident management," *Int. J. Med. Inform.*, vol. 79, no. 4, pp. e1–e17, Apr. 2010.
[37] 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.
[38] 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.
[39] R. Davison, M. G. Martinsons, and N. Kock, "Principles of canonical action research," *Inf. Syst. J.*, vol. 14, no. 1, pp. 65–86, 2004.
[40] K. Olesen and M. D. Myers, "Trying to improve communication and collaboration with information technology: An action research project which failed," *Inf. Technol. People*, vol. 12, no. 4, pp. 317–332, 1999.
[41] R. Taylor, "Interpretation of the correlation coefficient: A basic review," *J. Diagnostic Med. Sonogr.*, vol. 6, no. 1, pp. 35–39, Jan. 1990.
[42] M. Gibbert, W. Ruigrok, and B. Wicki, "What passes as a rigorous case study?" *Strategic Manage. J.*, vol. 29, no. 13, pp. 1465–1474, Dec. 2008.
[43] A. M. Riege, "Validity and reliability tests in case study research: A literature review with 'hands-on' applications for each research phase," *Qualitative Market Res., Int. J.*, vol. 6, no. 2, pp. 75–86, Jun. 2003.
[44] J. M. Morse, M. Barrett, M. Mayan, K. Olson, and J. Spiers, "Verification strategies for establishing reliability and validity in qualitative research," *Int. J. Qualitative Methods*, vol. 1, no. 2, pp. 13–22, Jun. 2002.
[45] 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.
[46] 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.
[47] J. C. Williams, "A user manual for the heart human reliability assessment method," DNV Technica, Oslo, Norway, Tech. Rep., 1992.
[48] National Patient Safety Foundation. (Jan. 2015). *RCA Improving Root Cause Analyses and Actions to Prevent Harm*. [Online]. Available: https://Www.Npsf.Org
[49] P. D. Hibbert, M. J. W. Thomas, A. Deakin, W. B. Runciman, J. Braithwaite, S. Lomax, J. Prescott, G. Gorrie, A. Szczygielski, T. Surwald, and C. Fraser, "Are root cause analyses recommendations effective and sustainable? An observational study," *Int. J. Qual. Health Care*, vol. 30, no. 2, pp. 124–131, Mar. 2018.
[50] *Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview*, Ponemon Inst., Traverse City, MI, USA, 2017.

MARK EVANS is currently pursuing the Ph.D. degree in information security with De Montfort University. He is also an information security professional with over 15 years 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 current 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 current research interests include cyber threat intelligence, security risk management, decision-making, business analytics, control systems architecture, and human's aspects of security. She also works on 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 has also been a joint Ph.D. Student with The University of Manchester. He is currently an Associate Professor with the Key Laboratory 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 current research interests include 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 was a leading Research Associate in Choice Architecture for Information Security (ChAISe) Project with 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. She has been a Senior Lecturer in computing science and cyber security with the Faculty of Technology, De Montfort University, Leicester, U.K., since 2016, where she is a member of Cyber Technology Institute. Her current research interests include multicriteria decision analysis and optimization and their application in various domains, including security, manufacturing, health care, and chemoinformatics.

HELGE JANICKE received the Ph.D. degree in computer science, in 2007, and involved in cyber security with organizations, such as Airbus, BT, QinetiQ, Ministry of Defence, and General Dynamics U.K. He is currently the Technical Director of Cyber Technology Institute, De Montfort University. He is also the Head of the School of Computer Science and Informatics. His current research interests include formal verification techniques and their application to cyber security, SCADA and industrial control system security, and aspects of cyber warfare. He established DMU's Airbus Group Centre of Excellence in SCADA Cyber Security and Forensics Research, in 2013. He is a 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.

EFPRAXIA ZAMANI received the Ph.D. degree from the Department of Management Science and Technology, Athens University of Economics and Business, Athens, Greece. She is currently a Senior Lecturer of information systems with the University of Sheffield. Her current research interests include intersection of organizational and social aspects of information systems, with an emphasis on postadoption user behavior, enterprise information systems, and blockchain applications. Her work has been presented in numerous journals, such as the *Journal of Information Technology*, *Government Information Quarterly* and the *International Journal of Electronic Commerce*.

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 is the author of more than 100 articles in scientific magazines and conferences.