HI-risk: A Method to Analyse Health Information Risk Intelligence

Prof William J Buchanan
Edinburgh Napier University, Edinburgh. UK
w.buchanan@napier.ac.uk

Dr Nicole van Deursen
Edinburgh Napier University, Edinburgh. UK

***Abstract*— Information security threat intelligence is a prevalent topic amongst researchers, long-established IT-vendors and start-ups. The possibilities of big-data analytics to security threat and vulnerability scanning offer a phenomenal development in the protection of infrastructures. At the same time, industry research reports continue to state that the main contributing factor in the events leading to a data breach is human error. The common response of information security professionals is to resort to technological solutions to prevent these human errors. However, some very important information security intelligence is not hidden within the network traffic: it's available from the people that work with sensitive information. This article describes the Health Information risk (HI-risk) method to identify non-technical information security risks in healthcare. The method includes risks related to skills, behaviour, processes, organisational culture, physical security, and external influences. HI-risk offers a solution to collect intelligence about non-technical information security incidents from across the healthcare sector to demonstrate past trends and to be ahead of future incidents. A test of a HI-risk forecast proved the feasibility of this approach in healthcare and beyond. It is suggested that HI-risk could become a valuable addition to existing technical threat and vulnerability monitoring tools.**

Keywords—risk model, security intelligence, socio-technical information security

I. INTRODUCTION

Information security concerns us all. Our digital identity is a valuable asset that we would like to protect. This may be even more important with our digital medical identity. We (as patients, as healthcare consumers, as family and friends of patients) need to have trust in the level of respect, protection and quality of care that information about us receives from the people and organisations with which we share it.

Advances in information technology have made it easier to provide and share health, especially medical, information, but at the same time have raised questions about information confidentiality, information integrity and unauthorised access (Appari & Johnson, 2010; Information Commissioner's Office, 2010; Meingast et al., 2006; Patientprivacyrights.org, 2013). It has been found that 90% of health care organisations suffer from data breaches (Ponemon, 2016), so

These issues could lead to consequences such as: patients avoiding care; embarrassment, stigma or discrimination; identity theft; medical errors; and disruptions in critical infrastructure. All of these could result in the loss of public trust in healthcare.

The Health Information risk (HI-risk) method expounded here aims to address this concern by identifying and sharing knowledge of information security risks. A previous publication described how the method was developed by means of a survey and a three-round Delphi study (Van Deursen, Buchanan, & Duff, 2013). That development stage produced an information security risk forecast. This article reports how the reliability of that forecast was tested within healthcare in the United Kingdom.

II. HI-RISK RELATED TO OTHER RISK AND INTELLIGENCE APPROACHES

Traditional risk assessment methods commonly start by setting a imaginable boundary around the assessed entity. However, security risks do not stop at organisational or system boundaries. The World Economic Forum (2016), which considers cyberattacks as a key economic risk, indicates that the growing cyber dependency across people, things, and organisations raises "the odds of a cyberattack with potential cascading effects across the cyber ecosystem. As a result, an entity's risk is increasingly tied to that of other entities" (p.18). For that reason, the HI-risk method does not analyse the risks of one healthcare organisation or system alone, but gathers risk data on a regional or sector-wide level.

Increasingly the traditional information security risk approaches are being shelved by organisations and replaced by cybersecurity intelligence tools. This intelligence is formed by international public and private partnerships and supported by tools that enable powerful data analytics and visualisation techniques, in order to present real-time 'evidence' of current cyber threats.

However, the intelligence based on technology threats alone may not be complete. Cybersecurity is a multi-disciplinary problem and threats do not originate solely from the Internet. Many real-time threats to secret or vital information come from social engineering, changes in society, or from unexpected uses of information technology, and are undetectable to intelligence tools.

Social relations with users, resource owners, and other actors who appear outside the boundaries of the entity influence information systems and their risks. For that reason we argue

that studies of information security risks should be approached from a socio-technical perspective.

In socio-technical approaches, it is believed that organisations should be designed as a balance between:

1. the technical subsystem (the technology to produce work but also the techniques, methods, configurations, procedures and knowledge used);
2. the social subsystem (employees, knowledge, skills, attitudes, values and needs, reward systems and authority structures); and
3. the environment (customers, suppliers, rules and regulations, which govern the relations of the organisation to society at large).

A disturbance in the harmony between the three subsystems could lead to security incidents. For instance, the security of the technical subsystem is created and challenged by the social subsystem through the acts of the users and is also influenced by the environmental subsystem through legislation and patients' demands. When a security incident affects a technical subsystem, the social and environmental subsystems can be affected as well: staff will not be able to perform their tasks, and patients will not receive the expected care.

The HI-risk method is based on the perception that threats in the technical subsystem, the social subsystem, and in the environment are all important factors to define information security risks. Yet, threat intelligence tools focus mainly on the technical subsystem. Therefore, the HI-risk method aims to complement technical risk intelligence tools by sharing and analysing non-technical security knowledge (from events in the social subsystems and the environment) amongst healthcare organisations.

III. The HI-risk model

Healthcare organisations usually register incidents and events for internal use. HI-risk provides the possibility to register the non-technical (social and environmental) incidents in a central system that is used by multiple organisations. The system analyses the incident scenarios and visualises the most frequent ones. These scenarios are presented to a group of experts in the field: security experts, information governance functions, risk managers, policy makers, and so on. These experts can express their opinions about the expected frequency of occurrence for the future and add new trends. The involvement of experts to identify and evaluate future risks and trends, is a proven method for scenario building and forecasting (Padma et al., 2009; Rowe & Wright, 2001). Their expectation is based on their experience, their knowledge of countermeasures, legislation and socio-political issues. The combination of incident knowledge from the past and expert expectations for the future forms a risk map. The map is the main deliverable of the HI-risk method, and healthcare organisations can use that to monitor their information security risks.

The HI-risk method gathers data about information security events from different sources, organisations and platforms in a central database. The database is based on a normalised classification of risk variables. The classification was created by the researchers by combining "a number of classic threat and vulnerability taxonomies known in security research (Howard and Longstaff, 1998; Parker, 1998) and is adapted to health care by adding health care specific terminology (Brann and Mattson, 2004; Asaro et al., 1999; Carthey and Clarke, 2010; Department_of_Health, 2010). Furthermore it integrates factors to measure cultural and society risks (Hofstede, 2001; Da Veiga and Eloff, 2010; Williams, 2004)" (Van Deursen, Buchanan & Duff, 2013 p. 32).

The highest level of the classification consists of five categories:

1. The threat (who initiates a risk, and where does it start?).
2. The method (what kind of action does the threat actor perform?).
3. The weakness (the weak spots in the organisation, processes or systems that the threat abuses).
4. The event (the result of the action).
5. The damage (the number of patient records affected by the event).

These categories are further detailed into sub-categories and elements. The elements are unique variables that may contribute to risks. They are derived from existing knowledge of information security risk variables, combined with earlier explained healthcare specific risk areas.

Figure 1, based on Van Deursen (van Deursen, 2014), illustrates parts of the classification of variables. The model is flexible to integrate other variables, such as variables that influence the technical subsystem (which are often registered in Security Incident and Event Management (SIEM) software in organisations).

IV. Case study data collection

Information security incident data was collected through a survey and a three-round Delphi study. During the development stage, the researchers requested data directly from NHS Health Boards and Care Trusts in Scotland and England through a Freedom Of Information request. They found that the returned incident registers contained some narrative information about incidents and a basic categorisation of cause and location. Eventually, 2108 incident scenarios were made anonymous and analysed. The top 5 most frequently occurring scenarios and the most disastrous scenario (affecting > 10,000 patient records) were presented to a panel of experts in a Delphi study. The Delphi process consisted of 3 rounds of questionnaires. After each round, the researchers provided an anonymous summary of the experts' forecasts, as well as the comments that they provided with their judgements. Each expert then could revise their earlier answers in light of the replies of other members of the panel.

The Delphi study resulted in a forecast of possible information security risks in healthcare, visualised on a risk map and scenario descriptions.

V. Case study test results

The forecast was tested in a large hospital in the UK and the test included interviews, observations, a documentation study, a survey, and a quantitative analysis of incident data.

A. Results from quantitative analysis of incident data

The security manager in the case organisation supplied an overview of security events registered by the IT service desk and a number of additional not IT-related incidents that were registered by the security manager in the timeframe covering the year that followed after the forecast.

The list of events in the case organisation was entered into the HI-risk database and analysed. For each variable, the relative frequency of occurrence was calculated. The distribution of frequencies in the events forecasted by the HI-risk database was compared with the distribution in the case organisation. Figure 2 illustrates a selection of the variables that showed a similar pattern in the forecast and in the case organisation. For instance, it was shown that many security incidents are related to internal employees, mistakes, and human weaknesses. Threats from outside of the organisation and incidents caused by technology were registered much less often than these employee related incidents.

The second analysis compared the incident scenarios of the case organisation with the forecast. The most important forecasted scenarios are presented in Table 1.

Table 1 Top 6 scenario descriptions

Scenario number	Description
1	An unattended asset goes missing: an employee, located on the premises, leaves an asset unattended and consequently the asset goes missing. The asset contains personal information of patients.
2	Password, user ID or access token sharing: an employee, located on the premises, shares his/her log on credentials leading to disclosure of patient information to an unauthorised person.
3	Email to unauthorised recipient: an employee, located on the premises, sends an email to an addressee unauthorised to access the patient data included in the text or attachment, and consequently discloses the personal details of patients.
4	Theft on the premises: the theft of assets from the premises, containing personal data from patients.
5	Procedure not followed: an employee, located on the premises, does not follow the formal procedures leading to disclosure of patient information.
6	Wrong privileges set: an internal employee located on the premises was given the wrong authorisations/privileges, causing disclosure of personal patient information to unauthorised persons.

Figure 3 illustrates that these scenarios occurred within the case organisation at a frequency very close to the expected frequency. One difference occurred with scenario 4 (theft of assets). The case organisation made a distinction in their incident register between burglary from the premises and assets that have gone missing for unspecified reasons. However, many other organisations find that it is often difficult to identify a missing asset as stolen or being lost. Often, these incidents are treated as a theft scenario. This was indicated by the expert panel as well as by the organisations that provided input for the HI-risk database. For that reason, a recalculation was done by treating scenario 1 and 4 as one scenario. After combining the two possible scenarios into one, the combined scenarios fell closer to each other. However, the case organisation does the right thing by investigating these incidents in depth and by separating the theft from the inattentive employee, as these events can only be prevented if it is clear why assets disappear.

B. Feedback on the method after interviews and observations

Semi-structured interviews and non-participative observations were held as a means to further improve the quality of the HI-risk method. The most important aim was to test the normalisation of possible risk variables, which forms the structure of the HI-risk database.

The Security Manager and two Information Governance leads were selected for interviews because of their knowledge of information governance and risk management processes, and their leading role in promoting secure behaviour amongst staff. The interviews were guided by a list of open-ended questions and more questions were created during the interviews. The interviewees were asked general questions about information governance and information security, about their approach to risk assessment and their opinion about the most important risks. During the interviews, new potential risk variables were identified and these were added to structure of the database. Furthermore, the research team gained more knowledge about daily information security routines, policies, risk assessment methods and organisational culture.

The aim of the non-participative observations was to test if any risk scenarios could be spotted and if so, how well they could be added to the HI-risk method. The goal was specifically not to audit staff or to report any potential incidents. The aim was to test the HI-risk classification of information security incident variables. Staff were observed in their daily routines, without disturbing them. Each potential

information security risk was noted and matched against the classification. All staff that was involved in the research were cooperating enthusiastically and even pointed out risks. This led to very useful improvements of the list of risk variables and the database structure. Specific socio-technical scenarios that lead to security threats such as mergers of hospitals and the integration of their IT systems, budget issues, or the trend of physicians to bring their own devices were added to the model.

C. Case study conclusion

The case study allowed benchmarking of social and environmental information security incidents of one organisation against the average in the healthcare sector. It showed that risk scenarios materialised as expected. Where differences occurred, these could be explained by circumstances or specific incident handling procedures, which in turn could be inspirational other organisations should these be shared through the HI-risk system. Most of the risks that were forecasted were related to the social subsystem. It was remarkable that neither the incident registers nor the expert panel identified events related to the environmental subsystem, indicating a possible lack of awareness of the relevance of these risks.

VI. CONCLUSION

The HI-risk method shows potential to improve the knowledge of patient records' security. The method showed reliability in benchmarking and forecasting socio-technical risk factors when records of past incidents from a large group of healthcare organisations are analysed. The challenge for future development will be found in the enhancement of underlying technology of the method, the integration with SIEM products, threat intelligence systems, and in the promotion of a cultural change to share information security incident registers and socio-technical security knowledge with each other, in order to create better care for sensitive patient information.

The HI-risk method indicates that organisations should not keep information security incidents as their secrets. By using this method, there is the possibility to step away from traditional information security risk assessment approaches, which are aimed at individual organisations and systems, and to contribute to the knowledge of information security risks industry-wide. The approach enables organisations to learn lessons from each other and to unite in the prevention of recurring information security breaches that could harm patients and the society at large.

Several recent changes in legislation and research publications indicate a wider interest in sharing information security intelligence. For example, the European Data Breach Notification Regulation for electronic communication service providers was further strengthened with specific rules in 2013 (European Commission, 2013 to ensure that in the event of a data breach, customers are informed, the authorities are notified and that the problem is solved at a pan-European level. In 2018, organisations in all economic sectors within EU member states will have share data breaches once the new General Data Protection Regulation becomes effective. The HI-risk system may be of help to healthcare organisations as part of their compliance programmes.

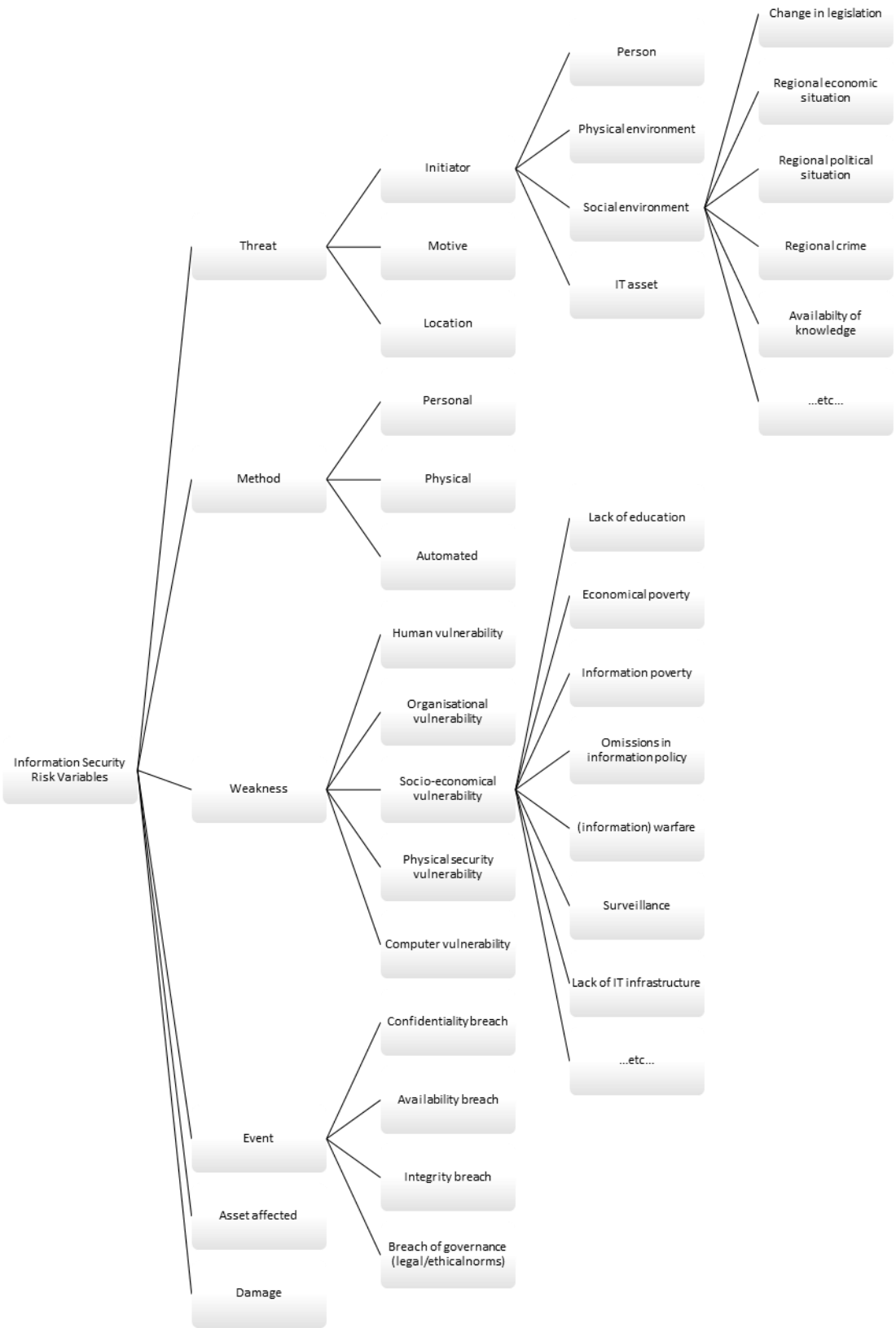

Figure 1. A selection from the classification of information security risk variables.

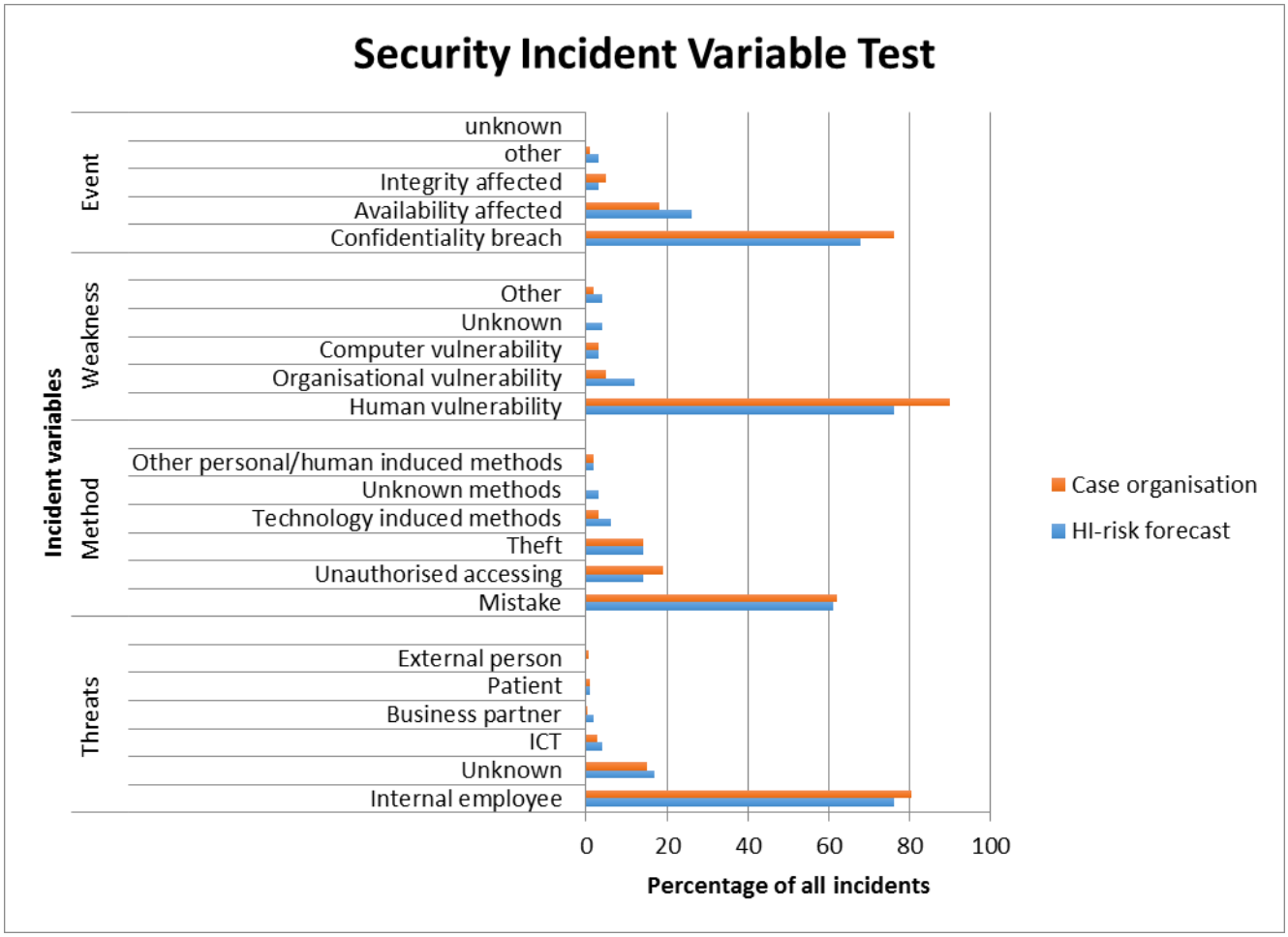

Figure 2 Security incident variable test

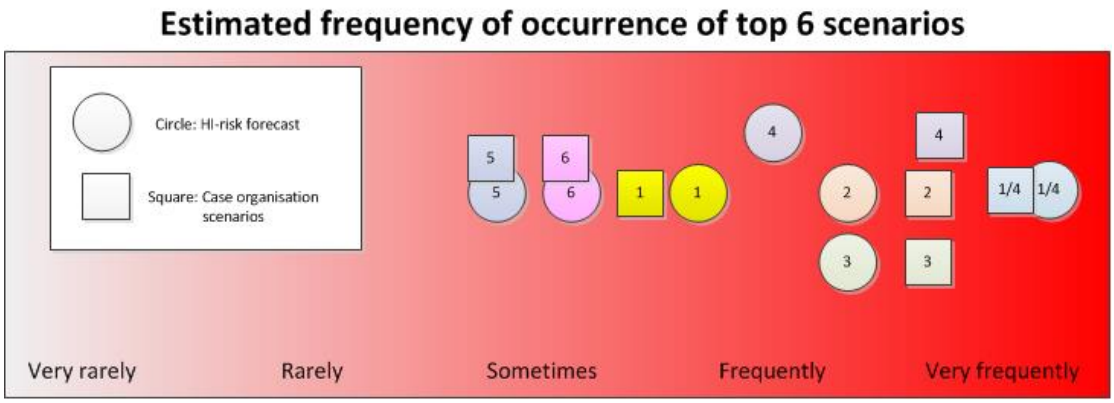

Figure 3 Estimated frequency of occurrence of top 6 scenarios

VII. REFERENCES

Appari, A. & Johnson, M. (2010). Information security and privacy in healthcare: current state of research. International Journal Internet and Enterprise management, 6(4), 279-310.

Asaro, P. V., Herting, R. L., Roth, A. C., & Barnes, M. R. (1999, November). Effective audit trails - A taxonomy for determination of information requirements. Paper presented at the Annual Symposium of the American Medical Informatics Association, Washington, D.C.

Brann, M., & Mattson, M. (2004). Toward a typology of confidentiality breaches in health care communication: an ethic of care analysis of provider practices and patient perceptions. Health Communication, 16(2), 231-251.

Carthey, J., & Clarke, J. (2010). Implementing human factors in healthcare. Patient safety first! Retrieved from Patient safety first website: http://www.patientsafetyfirst.nhs.uk/ashx/Asset.ashx?path=/Intervention-support/Human Factors How-to Guide v1.2.pdf.

Da Veiga A., & Eloff J.H.P. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207.

Department of Health (2010). Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents. Retrieved 1 October 2013 from http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/suichecklist.pdf.

European Commission. (2013). Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications. Retrieved 1 February 2014, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32013R0611:EN:NOT

Hofstede G. Culture's consequences. Comparing values, behaviors, institutions and organisations across nations. Thousand Oaks, California: Sage Publications; 2001.

Howard, J. D., & Longstaff, T. A. (1998). A common language for computer security incidents. Albuquerque and Livermore: Sandia National laboratories.

Information Commissioner's Office. (2010). Security Breaches reported to the ICO, V.6 15/06/2010. Retrieved 27 April 2011, from http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/breach_notification_spreadsheet.pdf.

Meingast, M., Roosta, T., & Sastry, S. (2006). Security and privacy issues with health care information technology. Paper presented at the 28th IEEE EMBS annual international conference, New York.

Padma, T., & Balasubramanie, P. (2009). Knowledge based decision support system to assist work-related risk analysis in musculoskeletal disorder. Knowledge-Based Systems, 22(1), 72-78.

Parker, D. B. (1998). Fighting computer crime. A new framework for protecting information. New York: Wiley Computer Publishing.

Patientprivacyrights.org. (2013). True stories. Retrieved 1 September 2013, from http://patientprivacyrights.org/true-stories/

Ponemon, 2016. http://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data

Rowe, G., & Wright, G. (2001). Expert opinions in forecasting: the role of the Delphi technique. In J. Armstrong (Ed.), Principles of Forecasting (pp. 125-144). Boston: Kluwer Academic.

van Deursen, N. (2014). HI-risk: a socio-technical method for the identification and monitoring of healthcare information security risks in the information society. (PhD thesis), Edinburgh Napier University, Edinburgh.

Van Deursen, N., Buchanan, W.J., & Duff, A.S. (2013). Monitoring information security risks within healthcare. Computers & Security, 37(September), 31-45.

Williams S.M., (2004). An international investigation of associations between societal variables and the amount of disclosure on information and communication problems: the case of Y2K. The International Journal of Accounting, 39(1), 71-92.

World Economic Forum. (2016). Global risks report 2016. Retrieved 28 July 2016, from: http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf

World Health Organization (2008). Global assessment of national health sector emergency preparedness and response. Retrieved 1 October 2013 from http://www.who.int/hac/publications/en/.