The true number of information security incidents is unknown, primarily as a result of under-reporting. Research from other disciplines on incident reporting can be reused to identify the critical success factors required to support an information security incident reporting model.

Why the Research?

It could be argued that in today's world information is ubiquitous and, increasingly for individuals, organisations and nations, seen as an asset which has value in its purest sense. It may be the case information has always been considered of value, as evidenced by early iterations of cyphers and encryption in Egyptian times, as well as Caesar cyphers and biblical cyphers (Singh, 1999). The main difference now being the sheer volume and accessibility of that information. An ever increasing proportion of that information is now stored, processed and accessed via technology and the reliance upon that technology and the skills to support it has become commonplace (Lockridge and Barnett, 2011) A collective noun 'Cyberspace[1]' commonly describes the widespread use and reliance upon the internet and it may be possible to consider cyberspace as an increasing element of a new engine of economic growth and, to some extent, a contributory factor to the modern industrial revolution as described by Jenson, (1993).

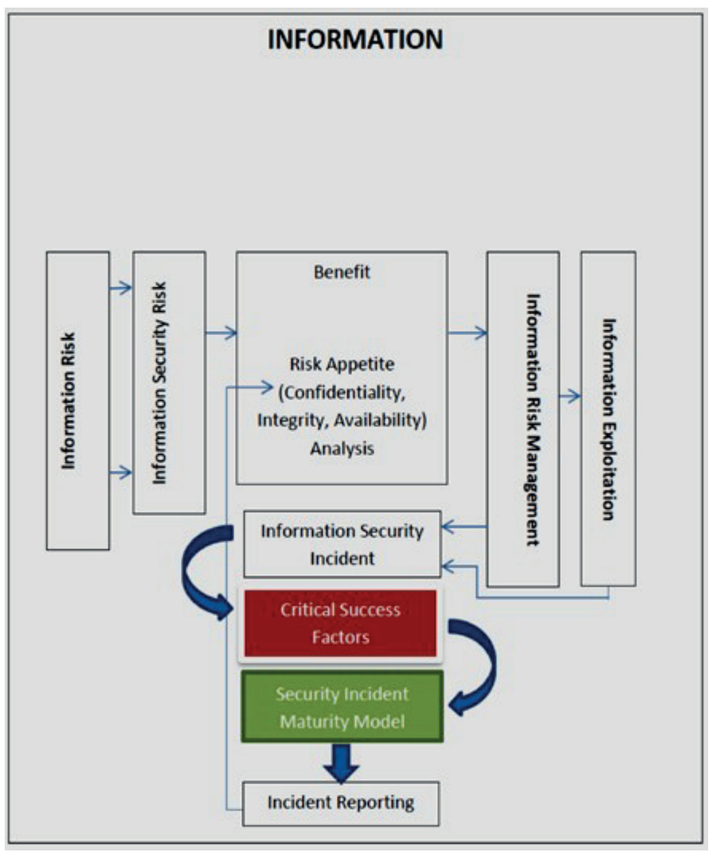
In this context there is a common perception amongst Information Security Professionals that the true number and type of information security incidents is unknown, mainly due to under reporting. Without empirical figures on reported incidents the accuracy and value of risk assessments is likely to be put into question.

If the real, or near real, picture of the likelihood of certain types of information security incident is not known, there is the danger that other more easily reported incidents such as system logs, IDS etc. are given higher prominence. These incidents logs, because they are tangible, can be used to justify risk based decisions. The absence of a wider perspective of the true nature of the type and volume of incidents and near misses may give undue prominence to electronic log indicators and may mask the real threat. Information security incidents that rely upon staff to report are equally important in assessing risk and it is the perceived lack of reporting of these that is thought to be of real concern.

1. Cyberspace. The notional environment in which communication over computer networks occurs. http://www.oxforddictionasries.com/definition/english/cyberspace last viewed 8/3/15

Information Risk Conceptual Framework

The below conceptual framework shows the flow from information risk to risk management, exploitation and information security incident occurrence. The perceived problem is there is a break in the logical flow when it comes to incident reporting. If significant numbers of incidents are not reported then the data upon which risk management decisions are made could be flawed. It is suggested that by identifying the critical success factors required to support better incident reporting and to develop an incident reporting maturity model based on those factors, the logical flow can be improved. This in turn potentially enables more empirically based risk decisions.



Literature Review

The literature review identified that little research in the reporting of information security incidents had taken place. In contrast, in the healthcare sector, there were numerous published papers and reports on 'adverse patient incidents' for example; Hui-Ying Chiang, PhD, RN; Shu-Yuan Lin, PhD, RN et al 2010, Lawton and Parker, 2002 and Firth Cozens, 2002. The healthcare sector literature also gives potential reasons why under reporting may have occurred. Incident reporting barriers were identified in the British report; Department of Health: An Organization with Memory (2000). There are a number of papers and studies on the efforts to share incident information between groups and sectors or on risk methods that comment on the lack of accurate data of reported incidents but none tackle the reason why. (Baskerville, R. 1991), (Baker, W.H., Rees L.P., Tippett, P.S. 2007).

It would therefore be valuable to obtain the opinion of information security professionals on the potential similarities in the barriers to reporting and learning from incidents that were identified in research in healthcare and elsewhere. Could the research be applicable and reused by the information security sector?

Selective References

Baker, W.H., Rees, L.P., Tippett, P.S. (2007) *Necessary Measures - Metric Driven Information Security Risk Assessment and Decision Making.* Communications of the ACM October Vol 50 No 10 Pages 101 to 106.

Baskerville, R. (1991) *Risk Analysis as a Source of Professional Knowledge.* Computers and Security, 10, 749-764 Elsevier Science Publishers Ltd.

Chiang Hui-Ying, PhD, RN; Lin Shu-Yuan, PhD, RN; Hsu Su-Chen, MBA, RN; Ma Shu-Ching, MSN, RN. (2010) *Factors determining hospital nurses' failures in reporting medical errors in Taiwan.* Nursing Outlook ;58:17-25. doi:10.1016/j.outlook.2009.06.001

Dalkey, N. (1969) *The Delphi Method: An Experimental Study of Group Opinion.* http://www.rand.org/content/dam/rand/pubs/research_memoranda/RM5888/RM5888.pdf last viewed 23/4/14

Department of Health: Organisation with Memory (2000). The Stationary Office ISBN 0-11-322441-9Firth-Cozens, J. (2002) Barriers to Incident Reporting, Quality & Safety in Health Care. British Medical Journal ;11:7, doi: 10.1136/qhc.11.1.7

JENSEN, M. C. (1993), The Modern Industrial Revolution, Exit, and the Failure of Internal Control Systems. The Journal of Finance, 48: 831–880. doi:10.1111/j.1540-6261.1993.tb04022.x http://onlinelibrary.wiley.com/enhanced/doi/10.1111/j.1540-6261.1993.tb04022.x/last viewed 9/3/15

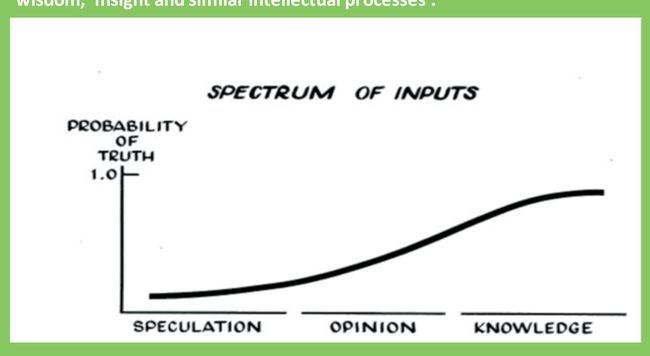
Lawton, R and Parker, D. (2002) *Barriers to incident reporting in a healthcare system.* British Medical Journal Quality Safety in Health Care 2002 11: 15-18. doi: 10.1136/qhc.11.1.15

Lockridge, B, Barnett, R (2011) Cyber Defence University of Pittsburgh eleventh Annual Freshman conference paper no. 2193

Singh, S. (1999). *The Code Book The Secret History of Codes and Code-Breaking.* Fourth Estate, Harper Collins London

Speculation versus Knowledge

Dalkey (1969, p2) refers to there being a spectrum of inputs; ranging from knowledge through to speculation. In between lies opinion which he believes is the flattering name for the collective 'products of judgement, wisdom, insight and similar intellectual processes'.



It could be argued that security incident reporting is at best sitting between

Pilot Study. Response of attendees at security conferences in 2011 to*; "What degree of confidence do you have in the number of information security incidents that are actually reported?"*

	All or the majority	*Some or few*
Public Sector	***35%***	***65%***
Private Sector	***47%***	***53%***

Delphi Study. A Delphi to identify the critical success factors to improve security incident reporting was conducted between Dec 2015 to May 2016 over two rounds. Consensus identified four critical success factors.

An Incident Reporting Maturity Model is in development prior to being subjected to a validation test

Mike Humphrey MSc F.Inst.ISP

Cranfield University, Defence Academy of the United Kingdom, Shrivenham, Swindon, SN6 8LA

m.humphrey@cranfield.ac.uk

www.cranfield.ac.uk