Are we managing the risk of sharing Cyber Situational Awareness?

A UK Public Sector Case Study

Michael Davies, Menisha Patel
Department of Computer Science
University of Oxford
Oxford, England
{michael.davies, menisha.patel}@cs.ox.ac.uk

***Abstract*—The development of effective cyber situational awareness, that makes a significant contribution to the decision making process around information risk management, is an important goal for organizations across all sectors. The sharing of such information between and within organizations is seen as a key security enabler. This paper considers a case study of a UK Public Sector organization. The aim is to establish if the decision to share cyber situational awareness has been taken from an information risk management perspective, and to examine whether or not the organization is suitably well-placed, to manage the consequences of information loss, occurring as a result of the sharing process.**

Keywords—cyber situational awareness; risk; consequence management

I. INTRODUCTION

In the light of the growing importance attributed to the sharing of cyber intelligence and situational awareness [1] in the fight against cyber-crime, some important questions have emerged. Do the organizations participating in this information sharing activity fully understand the risks associated with sharing information, that may include data associated with threats to, and vulnerabilities in their own infrastructures? And crucially, are the consequences of losing such information being effectively managed? This paper explores answers to these questions by providing an overview of a case study within a small to medium sized organization in the UK Public Sector. The organization will be a participant in the Cyber-Security Information Sharing Partnership (CiSP), and thus engaged in the sharing process. Given the perceived lack of empirical research in this area [1], the study will look to make the following contributions, using a combination of semi-structured interviews, and a table-top cyber exercise:

- Was the decision to join the CiSP underpinned by a formal risk assessment?
- Is there evidence that the potential consequences of the loss of associated cyber situational awareness data are being effectively managed?
- How would the organization cope with a significant data breach within the CiSP?

II. BACKGROUND

A. Sharing Cyber Situational Awareness

The sharing of cyber situational awareness has assumed great importance. This is evidenced in the US, by President Obama signing into law in December 2015, the Cybersecurity Information Sharing Act [2], and here in the UK by the establishment of the CiSP. The CiSP represents a voluntary, joint 'industry government initiative to share cyber threat and vulnerability information', and seeks to increase overall situational awareness of the cyber threats to business. It allows participating organizations and individuals, to engage in the exchange of cyber situational awareness in a 'secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information' [3].

B. Information Assurance in the UK Public Sector

In the UK, the provision of security of information and its supporting ICT infrastructures within the Public Sector is long-standing and well established, underpinned by a wide range of standards and literature. The Security Policy Framework (SPF) is the capstone document that provides overarching governance throughout, ensuring that a consistent approach to information assurance, driven from board level is undertaken [4]. The framework mandates a risk-based approach to Information Assurance (IA) with a Senior Information Risk Owner (SIRO) appointed in each organization, who is accountable and responsible for information risk across the organization. It is exactly this mandated consistency of approach to IA, that gives some weight to the argument, that the results of an individual organizational case study, may in this case, be an indicator of more general behaviors across the wider sector.

C. Managing the Risk

This research project outlined in this paper does not set out to question the importance of shared cyber situational awareness, or the role of the CiSP in its provision. The importance of both are well understood. Rather, the research examines whether or not the decision taken by the organization, to embark on a strategy of sharing cyber situational awareness, has been undertaken from a risk managed perspective. The consequences of the loss of cyber threat and vulnerability information about an organization's infrastructure have the

potential to be severe. The SPF mandates such an approach, stating that 'Risk management is key and should be driven from Board level. Assessments will identify potential threats, vulnerabilities and appropriate controls to reduce the risks to people, information and infrastructure to an acceptable level' [4]. Evidence of the application of the framework will be collected, analyzed, reviewed and reported on, in this study.

III. Method

A case study of a small to medium sized UK Public Sector organization will be undertaken. Initially the study will focus on the collection and analysis of any supporting risk management documentation associated with the decision to engage in the sharing of cyber situational awareness through the CiSP. Subsequently a review of information risk incident management policy and procedural documentation will be undertaken. This will support the execution of a 2-stage approach to the empirical research, that will utilize an initial set of qualitative interviews with relevant participants, followed by a table-top cyber incident management exercise.

A. Semi-structured interviews

The qualitative interview methodology selected for the initial phase of this research is a semi-structured interview based approach. The questions will be presented to a range of participants, involved in the decision making process associated with entering into the CiSP scheme, and the subsequent consequence management of this activity. Participants will receive a consistent set of questions, phrased in an open-ended way. These questions will enable the participants to contribute as much detailed information as they feel appropriate, whilst leaving scope for potentially new and relevant aspects that were not predetermined by the phrasing of the original question set. Following interview transcription, thematic analysis will be employed to attempt to identify patterned meaning across the range of data provided. This approach will follow a methodology developed in the Psychology Department at the University of Auckland [5].

B. Cyber Exercises

The second element of empirical study will consist of a cyber incident management table-top exercise, that will specifically examine how the organization copes with a hypothetical data breach within the CiSP. There is an awareness that empirical research of a quasi-naturalistic nature has been limited to date [1], with such activity predominantly taking place within the realm of the military, as for example in the study undertaken by Malviya et al [6]. This exercise will be designed to closely examine the approach to the consequence management of a cyber incident. All UK Public Sector organizations are required under the SPF to have 'polices in place for reporting, managing and resolving any security incidents' [4]. The scenario will involve a significant loss of data, and the monitoring of the interactions between key players involved in the risk management of such an occurrence. An assessment will be made of the effectiveness of the consequence management plans and procedures in-place, that directly support the cyber situational awareness sharing activity.

C. Analysis

Thematic analysis, given its flexibility and utility, will be employed to identify patterns across the range of data provided by the participant consultants. Coding and theme development will be used to draw out the recurring and relevant themes in participant responses. Participant activity during the exercise will be video recorded, and the interactions between participants will be analyzed. The response to the simulated information security incident will be assessed in the light of extant risk management policies and procedural documentation, where appropriate. A post-exercise report will be generated following the exercise, which will be shared, with the participating organization.

IV. Conclusions and Future Work

It is the contention of the author, that this case study will provide important empirical evidence towards answering the question of whether or not effective risk management processes underpin decisions taken, to support the sharing of cyber situational awareness between organizations. Given that organizations in the UK Public Sector are mandated, under the SPF to adopt a risk-managed based approach to information assurance, an identified failure to do so in the target organization may be symptomatic of a wider failure across the sector. This will provide the impetus for further empirical research in this area which could subsequently be expanded to include organizations in the private sector.

References

[1] U. Franke and J. Brynielsson, "Cyber situational awareness – a systematic review of the literature," *Comput. Secur.*, vol. 46, p. 41, 2014.

[2] US Congress, "S.754 Cybersecurity Information Sharing Act of 2015." [Online]. Available: https://www.congress.gov/bill/114th-congress/senate-bill/754. [Accessed: 22-Feb-2016].

[3] CERT-UK, "Cyber-security Information Sharing Partnership (CiSP)," 2014. [Online]. Available: https://www.cert.gov.uk/cisp/. [Accessed: 22-Feb-2016].

[4] Cabinet Office, "HMG Security Policy Framework," *Security*, 2014. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf. [Accessed: 22-Feb-2016].

[5] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual. Res. Psychol.*, vol. 3, no. May 2015, pp. 77–101, 2006.

[6] A. Malviya, G. a. Fink, L. Sego, and B. Endicott-Popovsky, "Situational Awareness as a Measure of Performance in Cyber Security Collaborative Work," in *2011 Eighth International Conference on Information Technology: New Generations*, 2011, pp. 937–942.