# Organizational Vulnerability to Insider Threat

## What Do Australian Experts Say?

Justine Bedford(✉) and Luke Van Der Laan

The University of Southern Queensland,
Toowoomba, Australia
justine@jconsulting.net.au,
luke.vanderlaan@usq.ed.au

**Abstract.** Approaches to the study of organizational vulnerabilities to intentional insider threat has been narrow in focus. Cyber security research has dominated other forms of insider threat research [1]. However, within the scope of cyber security, the effort is predominantly focused on external threats or technological mitigation strategies. Deeper understanding of organizational vulnerabilities influencing insider threat and responses to insider threats beyond technological security remains limited in Australia. Despite the increasing potential threat and impact of such risk to organizations, empirical studies remain rare. This paper presents an initial study related to identifying organizational vulnerabilities associated with intentional insider threat. A Delphi Method was employed as part of a broader mixed methods study. There was a strong consensus amongst Australian experts as to the primary organizational vulnerabilities to insider threat. These main risks extend across personnel, process, technological and strategic (resource allocation) domains. The organizational vulnerabilities identified by Australian experts is consistent with research, literature, and guidelines, available from other countries. The results confirm the need to look beyond the narrow focus on individuals and technology in order to fully address the insider threat problem. Whilst only preliminary results are presented here, future analysis of data will focus on identifying best practice solutions for the Australian market.

**Keywords:** Insider threat · Organizational vulnerability · Cyber threat · Risk management · Technological security

## 1 Introduction

Insider threat has been defined as "…any activity by military, government, or industry employees whose actions or inactions, by intent or negligence, result (or could result) in the loss of critical information or valued assets" [2]. The behaviours associated with insider threat include espionage, sabotage, theft and terrorism [2, 3].

Studies of organizationally enabled insider threats are rare. Historically, research on insider threat has predominantly focused on individually motivated behaviour, psychological predispositions and technological weaknesses. This predominant research


C. Stephanidis (Ed.): HCII 2016 Posters, Part I, CCIS 617, pp. 465–470, 2016.
DOI: 10.1007/978-3-319-40548-3_77

provides a narrow perspective of examining insider threat within the context of organizational vulnerability due to architecture, structure, and processes. The reason for this is most probably a result of underreporting by organizations due to a fear of loss of reputation [4]. It may also be a way to place blame on an individual or technological failure, rather than focus on organizational control and responsibilities.

In the cyber security space, research has concentrated on computer hackers, disgruntled employees, ex-employees and consultants [5]. The research has rarely provided any organization-wide recommendations or managerial decision-making tools as a means for developing countermeasures [1] due to organizational vulnerability as the source of cyber threat. However, researchers are increasingly calling for further studies related to security efforts that account for individual, social, and organizational influences, and that risk management must extend beyond the almost entirely technological detection solutions currently in place [4]. Whilst research to date has been useful it has ignored or undervalued broader organizational dimensions that increase and decrease insider threat.

Colwill [6] confirms that a focus on cyber security and information technology alone does not provide a balanced solution. Certainly this is true when taking into account that insider threats are viewed as more damaging than external threats. Insiders can circumnavigate technical detection and technical detection mechanisms are limited to post-hoc identification of actual insider threat activity [7].

Whilst security is improved by technological assistance and advancement it is not enough [8]. Employers become comfortable and perhaps over reliant on technology. The result is usually missing opportunities to embrace other proactive forms of addressing the insider threat phenomena, including human factors, education and awareness, and crisis response [6].

Given the current status of research on insider threat there is potential to expand understanding of the phenomenon including organizational predispositions and vulnerabilities [9]. This is important as Festa [10] noted that the overall body of research on insider threat is biased, insufficient, and lacking. In summary, the spectrum of insider threat research should embrace a holistic approach that reflects the complexity and convergence of variables that result in damage.

Further attention to broader government, private sector and not-for-profit organizations is warranted especially given that global relevance of research and collaboration has been limited [10]. This is especially clear in Australia where there is a lack of published work and research available in the public and practice domain.

This preliminary study aims to begin addressing some of these limitations in research in the Australian context. It looks to broaden the scope of available research by (a) considering Australian expert opinion, (b) gathering information across private and public sector organizations, (c) providing a diverse focus across individual, organizational, and technological vulnerabilities and (d) identifying first and second-tier mitigation techniques that extend beyond information systems and contribute to warning indicators (although this last point is not addressed in the current poster presentation).

## 2 Methodology

If insider threat risks are statistically rare [3] or more likely, seldomly reported, then quantitative methods alone cannot provide a full picture of such behaviour. As such the inclusion of qualitative methods, through information provided by subject matter experts is one way to gather relevant and purposeful information on insider threat [1].

The Delphi Method was chosen as an appropriate means of gathering expert opinion through a multi-stage email questionnaire. The Delphi method is an attractive method for researchers as it is a flexible research technique that is suited to addressing problems or phenomenon where limited information exist [11]. It also allows for equality of response thus avoiding dominant (usually prevailing) opinion and allows experts to change their responses. It is a versatile method for exploratory study [12], as is the case with insider threat, where the topic is delicate, sensitive or undocumented [13].

Use of expert opinion in studying insider threat is well established [1, 14]. Consistent with the themes addressed by Okoli and Pawlowski [12] a Delphi Method is considered the most practical and applicable research method as it can investigate a complex issue, provide a group method where experts do not need to meet, is a flexible design that allows for follow up (leading to richer data/deeper understanding), can allow for solicitation of information and, as in this study, ranking importance of organizational vulnerabilities. It also provides a group opinion which may be more valid than an individual opinion [15].

### 2.1 Choosing Delphi Participants/Experts

For the purpose of the current study, experts were selected based on demonstrated expertise in the field of insider threat and specifically targeted to ensure coverage of the private and public sectors. In addition to at least 10 years of involvement in Justice, National Security, Crisis Management, Counter Intelligence, Cyber Security, Risk Management, and Fraud Investigation, experts also had to meet one of the following recruitment criteria: (1) postgraduate qualifications in insider threat related research, (2) published articles on insider threat or related phenomena, (3) involvement in investigating insider threat cases, or (4) involved in the assessment and mitigation of insider threat within organizations. As such, the experts may be employees or employers or subject matter experts with relevant commentary on insider threat. Given the narrow field of expertise the group was an homogenous sample.

### 2.2 Participants

The use of convenience sampling and snowball techniques are commonplace in research employing the Delphi method [15]. Using these methods, email requests were sent out to 28 experts inviting participation. Of the 28 experts who were contacted to participate in the study, two declined participation, nine did not respond to the email, and 17 consented to participate in the research. To attempt to enhance participation, follow-up emails were sent to those who had not responded to the initial request for

participation. After emailing the first round of the Delphi, two experts withdrew from the process. This left a total of 15 experts participating in round 1 of the Delphi study. Attrition did occur, but was minimal (13 %).

### 2.3 Delphi Items and Process

The items of the initial Delphi questionnaire were guided by literature review findings. These items were considered to be of high pertinence [15] and the expert panel were required to give feedback and make judgements on these pre-selected issues (on a five-point Likert scale and through free text responses). Experts were also offered the opportunity to raise issues and ideas not already identified in the questionnaire. The questions of the Delphi rounds aimed to gain insight into (1) the experts understanding and definition of insider threat, (2) what organizational vulnerabilities they believe contribute to insider threat behaviour, and (3) how organizations can better protect themselves from insider threat. This paper focuses on point 2 - the organizational vulnerabilities that Australian experts believe contribute to an increased risk of insider threat.

## 3 Results

Descriptive statistics and P-P Plots were used to assess the responses from the Australian panel experts and determine the level of consensus reached and the identification of any emerging issues or major discrepancies. Consensus on a question was deemed to be achieved if a) at least 70 percent (typically acceptable in Delphi research - see Brewer [16]) of panel members agreed on the direction of the response and b) there was no abnormal distribution of responses i.e. normal distribution, with a low variability and minimal outliers. Where any item achieved at least 70 % agreement and there were no 'polar-opposite' responses of concern it was considered to have reached consensus and eliminated from the next round. This helped reduce the length of subsequent rounds which is also considered a method of reducing attrition in expert participation [15].

Classical content analysis of qualitative data was used to determine emerging themes from responses to open ended questions in rounds one and two of the Delphi. Based on these analytical techniques the panel demonstrated a high level of consensus across the questions during the three rounds of the Delphi Method.

The themes of vulnerabilities were then reviewed to determine those that were of primary importance - where more than 90 % of panel experts agreed or raised an issue/idea and at least one third strongly agreed with that vulnerability. Based on the analyses completed the following were considered primary weaknesses and vulnerabilities that, according to Australian experts, increase the likelihood of insider threat (Table 1).

**Table 1.** Primary vulnerabilities that increase the likelihood of insider threat

| | |
|---|---|
| People | 1. Ego/sense of entitlement<br>2. Disgruntlement<br>3. Ethical flexibility<br>4. Increase in staff counterproductive workplace behaviour/workplace deviance |
| Process | 5. Poor security practices of leadership<br>6. Poor application of security<br>7. No consequences for poor security behaviour |
| Technological | 8. Limited/no auditing and monitoring capabilities<br>9. Lack of electronic access controls |
| Strategic | 10. Lack of strong and well-defined organizational culture |

## 4 Conclusion

Based on Australian expert opinion, ten primary organizational vulnerabilities that increase the likelihood of insider threat have been identified. These vulnerabilities extend across organizational domains, consistent with research suggesting that addressing insider threat requires more than a narrow focus on technology and/or individual solutions (e.g. [6]). The findings are consistent with previous published works noting that insider threat is a multi-disciplinary concern [8, 17] and demonstrate that organizations need to consider people, process, technology, and organizational strategy in order to adequately address and reduce their risk of insider threat. The latter is closely associated with a leadership predisposition to allocate resources to counter insider threat as a key strategic priority.

It is confirmed that focusing on cyber security and information technology alone does not provide a balanced solution [6] and that broader focus to include weaknesses in the organizational context must be further studied. As Colwill [6] suggested embracing other proactive forms of addressing the insider threat phenomena is necessary. The outcomes of this study suggest that at a minimum a focus on organizational culture and security application and practices must also be part of an overall insider threat solution.

In order to develop a greater understanding of insider threat in Australia, further analysis of the Delphi Method data will be undertaken. Such analysis will provide Australian expert opinion on the top organizational methods and strategies to help decrease the likelihood of insider threat. In the future it is hoped that the Delphi Method information will be distilled into strategies for organizational best practice for the prevention and mitigation of insider threat based on Australian expert opinion.

## References

1. Catrantzos, N.: Managing the Insider Threat: No Dark Corners. CRC Press, Boca Raton (2012)
2. Shaw, E.D., Fischer, L.F., Rose, A.E.: Insider risk evaluation and audit (2009). http://www.dhra.mil/perserec/reports/tr09-02.pdf. Accessed 21 June 2014

3. Shaw, E., Fischer, L.: Ten tales of betrayal: the threat to corporate infrastructures by information technology insiders: analysis and observations (2005). http://www.dhra.mil/perserec/reports/tr05-13.pdf. Accessed 21 June 2014
4. Willison, R., Warkentin, M.: Beyond deterrence: an expanded view of employee computer abuse. MIS Q. **37**(1), 1–20 (2013)
5. Brackney, R., Anderson, R.: Understanding the insider threat (2004). http://www.rand.org/pubs/conf_proceedings/CF196/index.html. (cited 22 June 2014)
6. Colwill, C.: Human factors in information security: the insider threat - who can you trust these days? Inf. Sec. Tech. Rep. **14**, 186–196 (2010)
7. Maasberg, M., Warren, J., Beebe, N.: The dark side of the insider: detecting the insider threat through examination of dark triad personality traits. In: 48th Hawaii International Conference on System Sciences, Hawaii, USA (2015)
8. Cappelli, D.M., Moore, A.P., Trzeciak, R.F.: The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Pearson Education, Upper Saddle River (2012)
9. Band, S.R., et al.: Comparing insider IT sabotage and espionage: a model-based analysis. DTIC Document (2006)
10. Festa, J.P.: New technologies and emerging threats: personnel security adjudicative guidelines in the age of social networking. DTIC Document (2012)
11. Skulmoski, G., Hartman, F., Krahn, J.: The Delphi method for graduate research. J. Inf. Technol. Educ. **6**, 1–21 (2007)
12. Okoli, C., Pawlowski, S.: The Delphi method as a research tool: an example, design considerations and applications. Inf. Manag. **42**, 15–29 (2004)
13. Lilja, K.K., Laakso, K., Palomaki, J.: Using the Delphi method. In: 2011 Proceedings of PICMET 2011 Technology Management in the Energy Smart World (PICMET) (2011)
14. Greitzer, F.L., et al.: Psychosocial modeling of insider threat risk based on behavioral and word use analysis. e-Service J. **9**(1), 106–138 (2013)
15. Keeney, S., McKenna, H., Hasson, F.: The Delphi Technique in Nursing and Health Research. Wiley, Hoboken (2010)
16. Brewer, E.: Delphi technique. In: Encyclopedia of Measurement and Statistics. Sage Publications Inc, Thousand Oaks (2007)
17. Nurse, J.R.C., Legg, P.A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M., Creese, S.: A critical reflection on the threat from human insiders – its nature, industry perceptions, and detection approaches. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 270–281. Springer, Heidelberg (2014)