THERE IS NO SINGLE SOLUTION TO THE 'INSIDER' PROBLEM BUT THERE IS A VALUABLE WAY FORWARD

DANIEL BILUSICH, LEUNG CHIM, RICK A. NUNES-VAZ & STEVEN LORD
Defence Science and Technology, Australia

ABSTRACT

The threat posed by insiders deliberately or inadvertently misusing their knowledge and access to sensitive information is a major security challenge. Finding effective, acceptable and affordable ways to manage the insider threat is non-trivial, involving the use of controls that range from technical to procedural. To make matters worse, insider activities range from inadvertent or accidental disclosure, through deliberate damage caused by disgruntled employees, to the pre-positioned mole who may undermine the organisation's viability or purpose. The same controls will have different levels of effectiveness for each of these insider types. Based on these factors, attempting to find a single, optimised, universal solution to insider threats is illogical. However, the literature still contains statements such as 'deterrence is the best approach for insiders'. There are dangers for security managers in drawing broad conclusions across the insider threat spectrum based on statements like these. Insider threats typically have a distribution of incidents where there are many of small consequence coexisting with a small number of incidents with very large consequences. This suggests that risk management techniques are a relevant, and arguably the most appropriate, framework for insider management. We have developed and applied a risk-based framework to model the spectrum of insider threat types, to enable the decision maker to determine the relative security effectiveness of alternative solutions. It allows decision makers to prioritise security investment to achieve the greatest benefit-cost using residual risk as the performance metric. Our framework provides a traceable and accountable method for organisations to balance their investments in controls, according to the complex spectrum of insider activity they are dealing with. They may also extend the approach, using robust analysis, to manage their uncertainties. Our framework supports security managers in customising security for their organisation based on its unique requirements.

Keywords: insider threat, risk management, risk-based framework, investment prioritisation.

1 INTRODUCTION

The threat posed by insiders deliberately or inadvertently misusing their knowledge and access to sensitive information is a major security challenge [1]. By virtue of their privileged status, trusted insiders are able to exploit vulnerabilities created by their legitimate access to sensitive information, as well as those created by failures of effective internal security implementation. While the incidence of insider misuse may be lower than that of attacks from outside the organisation, their consequences are generally more serious [2]–[5]. It has been estimated that on average each insider incident costs in excess of $400,000; and there have been multiple incidents with losses exceeding $1 billion [6]. The examples of Bradley Manning and Edward Snowden [7] demonstrate the impacts that can occur when insiders choose to disclose highly sensitive information.

The insider literature is extensive, with a significant portion [8] describing specific controls or countermeasures that are suitable for combating insider threats [9]–[14]. These references are a good starting point for security managers to determine what options are available for them to apply when improving their organisation's security system. Controls for insiders range from physical and technical to behavioural and organisational [1], [15] but are becoming increasingly sophisticated as technology and understanding evolve. A more extreme example being the potential to use human bio-signals (electroencephalography – EEG) by applying an EEG on all staff as an intent-based access control system [16], [17].

WIT Transactions on Engineering Sciences, Vol 121, © 2018 WIT Press
www.witpress.com, ISSN 1743-3533 (on-line)
doi:10.2495/RISK180121

Many of the controls described in the literature are deterrence, detection or prevention techniques and the majority focus on addressing malicious insiders only, such as the EEG example described above [16], [17]. Although there is no problem with this, it is important for us to acknowledge that insiders can vary across a spectrum, from the careless insider to the implanted mole. This is important as the effectiveness of controls is likely to vary based on the type of insider exposed to them. There is currently no universally accepted taxonomy of the insider threat; however, a number of classifications [13], [15], [18], [19] and definitions [1], [13], [20] are available. Security managers will most likely need to consider the variations across the insider categories when making informed decisions on their security arrangements: it being unlikely that only one type is potentially active in any given context.

We therefore consider three types of insiders as we progress through this paper; the careless insider (who unintentionally compromises security), the disloyal insider (who entered the organisation as a loyal employee but whose attitude subsequently changed) and the mole (who entered the organisation with the deliberate intent to cause great harm and/or to benefit an external agent).

To assist security managers, identify the opportunities they have to control insiders, insider threat pathways (or kill-chains or attack vectors) have been developed to reveal the general steps an insider follows to achieve their objectives [6], [13], [19], [21]–[25]. An example of a threat pathway for a malicious insider is shown in Fig. 1. It also identifies (in blue) the nature of interventions intended to prevent security breaches or protect the targets of such breaches. A framework for how to disaggregate pathways into more detailed steps is also available [23] and may be useful to pinpoint where specific controls should be emplaced along the threat pathway. Although our assessment of the literature indicates that most favour describing preventative controls to stop the occurrence of a security breach, by assessing the threat pathways (Fig. 1) it is clear that there is also an opportunity to potentially reduce consequences when a security compromise has occurred.

The insider threat is complex (with different threat types and various threat pathways to consider) and with so many controls available, the task for the security manager to select the best security package to implement is very difficult. Insider security strategies, or approaches, have been developed to guide the security manager's focus in order to achieve a stronger security system as a whole [6], [13], [26]–[35]. Generally, they describe where along the threat pathway the opportunity to stop the perpetrator is greatest, what sets of controls working together are most effective, or whether the focus should be specific types of controls (such as controls that achieve deterrence) over others (that target prevention as an example).

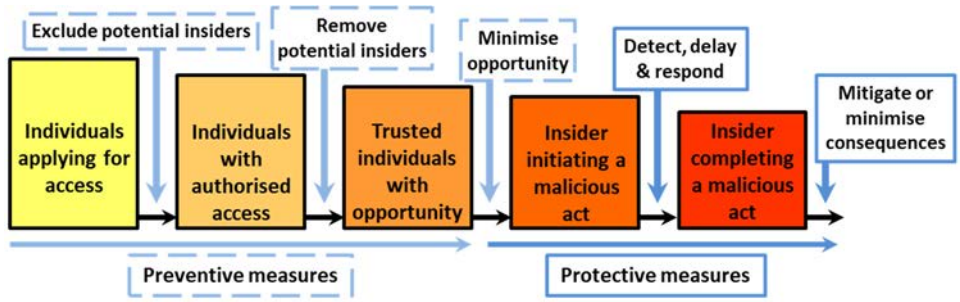

Figure 1: Exemplar of the insider threat pathway from origin of the insider threat to end impacts for the organisation, and how controls or interventions work along it. *(Source: IAEA, 2008 [21]; Duran et al., 2009 [22].)*

However, upon close examination of these strategies (we summarise several below), we identify some limitations that must be taken into account by the security manager when deciding which approach to implement.

One of the strategies is based on experience within the FBI where they identify the disgruntled insider as the largest (numerically) of insider threat types [6]. They advocate that deterring would-be perpetrators is a more effective strategy than monitoring their behaviours and detecting inappropriate actions. For this reason, they advocate creating an environment that discourages insiders.

Another strategy, in this case targeting the higher-level activity of a mole, is called 'No Dark Corners' [30], and it advocates empowering workers at the team level to deter, detect and intervene.

According to Cole and Ring [27], detection of significant security breaches is crucial. They argue that an organisation's efforts to prevent inappropriate insider activity is reasonably likely to stop the unsophisticated or weakly-motivated insider but is unlikely to stop a determined or sophisticated attacker, which they note is the type that causes the most damage to an organisation. For these insiders, they advocate an approach that focuses on detection of attacks, and information or evidence gathering sufficient to control the damage and prosecute the perpetrators. This approach contrasts with others by being generally reactive and focuses on security controls that work in the post-breach event timeframe.

Another approach in [28] is based on General Deterrence Theory [36], [37] where the aim is to maximise the effectiveness of deterrence and prevention in order to minimise the need for post-event detection and prosecution. The model strengthens deterrence by making potential offenders keenly aware of the consequences of inappropriate activity.

In our review, we note that some authors were quite clear about the range of insider types that their approach was targeting, and it was apparent that different security philosophies were needed to address different parts of the insider threat spectrum. Others unfortunately were less clear, and it remained ambiguous as to whether they intended their advice to be generally applicable across the whole spectrum of threat types, even though there is no single, universal solution. We suggest that security managers be cautious about adopting a particular security strategy without testing its value across the spectrum of insiders their organisation faces. We also note in the cited approaches above, that some of the advice is inconsistent. If we assume that they cannot all be correct, how does the security manager identify which approach to apply to achieve the greatest benefit-cost for their security investment? For those that advocate a multi-methodology approach [11], [28], how does the security manager determine which strategies deserve investment, and in what relative balance?

To answer these questions, we need a framework that allows the security manager to test the relative effectiveness of alternative security strategies (and combinations) against a variety of insider types. This would enable them to prioritise their investments and to customise their security arrangements to meet the organisation's needs. Security arrangements should be guided by a conceptual framework that takes account of the insider category, as well as the way that security controls interact to reduce insider risk along the threat pathway [15], [22], [31], [38]. Low incidence rates combined with high potential impact suggest that risk management techniques are a relevant, and arguably the most appropriate, framework for insider management [15], [22], [31], [39].

In the remainder of the paper, we address these issues through the use of a risk-based framework called Security-in-Depth (SiD) [40]. SiD was originally developed to support investment decisions in the physical security domain [41], [42], but was then extended and applied to address all national security threat types [43] and more recently to explore Defence's needs in building cyber security capability [44].

We begin by providing a brief introduction to the security in depth approach, and then apply it to a hypothetical insider problem in which the security manager is presented with two alternative security upgrade philosophies – one focused on strengthening behavioural compliance, the other on monitoring technologies – in order to highlight how each performs against three insider threat types from the spectrum. Our illustration is intended to show how security managers might adapt the method to suit their own needs.

2 SECURITY-IN-DEPTH

SiD [40], [43] was developed to compare physical security system effectiveness and to support investment decisions by prioritising controls that have the greatest potential for risk reduction. SiD is built on the concept of layered security where security layers can be applied to target specific parts of the threat kill chain. By having multiple layers, the perpetrator must defeat each security layer to be successful. Or from the security perspective, there are multiple opportunities to stop the perpetrator and so long as one layer is able to do so, the threat is defeated. Although the concept of multiple security layers is not new, what SiD has been diligent to provide, is to clearly define a security layer as an integrated collection of controls that can potentially stop a defined event from occurring or can eliminate its consequences [40].

Each layer is independent from other layers and the effectiveness of each layer can be evaluated. This is a critical aspect of SiD that can be used to support prioritisation decisions and will be demonstrated in the following section. A layer is composed of one or more functions which are performed by integrated sets of security controls serving a common purpose. Security controls can range from physical, technical, psychological, to procedural. The hierarchy of similar controls contributing to perform a specific function, and several interdependent functions working together to achieve a complete security layer is shown in Fig. 2.

As an example, if the risk event is a trusted insider stealing a physical copy of a classified report, then random personnel searches of staff on exit from premises (a procedural control) and a ‘tattle-tape’ magnetic strip system concealed in the cover of the report (a technical control), can both serve to detect potential insiders removing classified material. Detection is a security function and these two controls are both examples of controls that can perform that function. However, detection is not a security layer as on its own it is not sufficient to stop the perpetrator. Detecting removal of classified material requires additional functions such as responding to the detection to prevent consequences, which could involve apprehending the perpetrator to recover the document or changing operational practice so that the information in the document is no longer relevant. In such a case a package of controls that detect and respond are needed to create a layer.

In SiD, the threat attack is modelled as a critical pathway of sequential steps leading to the risk event, followed by fallout steps that generate the undesirable consequences and potential impact (Fig. 3). SiD exposes seven types of layers. The “Shape”, “Deter” and “Prevent” layers influence the likelihood of a risk event taking place while “Protect”, “Contain” and “Recover/Adapt” are layers which influence the consequences and impacts where a risk event has taken place. “Investigate” is a layer which involves the accumulation of evidence based on previous successful, failed or aborted acts, or from suspicious or modified individuals’ behaviour. As it generally works in slower time and is therefore an ongoing layer, the investigate layer is most likely to stop future events occurring after a series of previous acts.

The Shape layer is about screening potential insiders before they join the organisation or influencing the mind state of potential perpetrators so they do not develop intent to commit

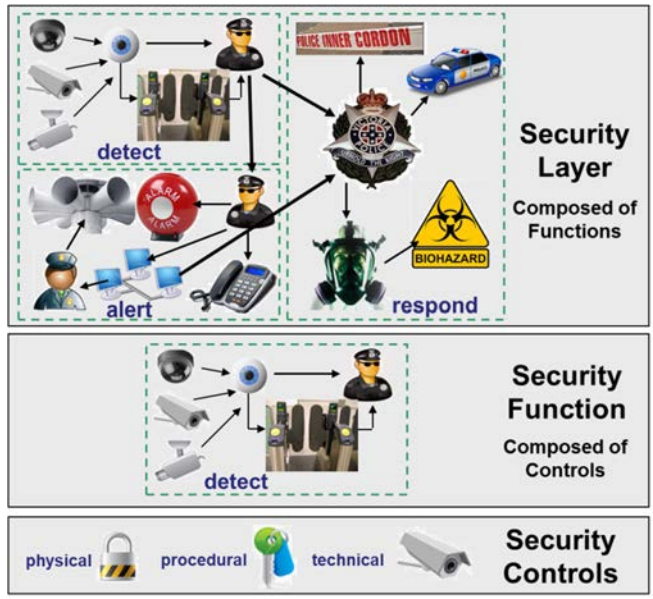

Figure 2: Only a security layer can reduce risk by reducing the likelihood or consequence of a risk event. Layers are composed of functions, which are collections of security controls that perform a similar role, such as detect, alert or respond. All functions are needed to create an effective layer. A security layer is independent of other layers as it contains all the integrated controls needed to reduce risk.

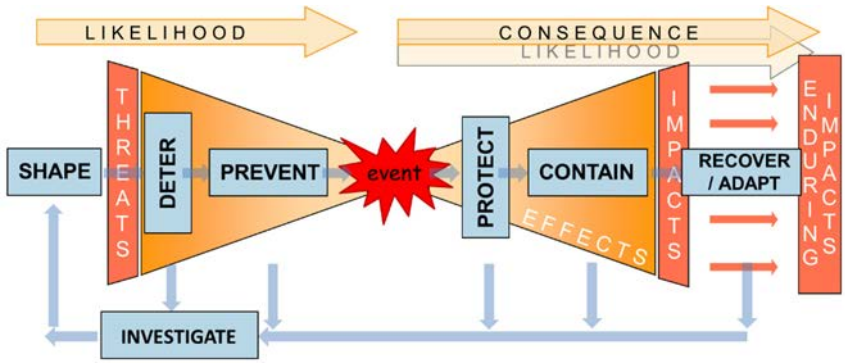

Figure 3: Security-in-depth approach of layers along a risk pathway abstracted by the risk bow-tie.

harm to the organisation. Where an insider does develop malicious intent, before they commit any act they may plan their act and weigh up the costs and benefits to them of progressing with their plan. The Deter layer refers to a collection of controls which work to stop someone with intent from pursuing their plan to achieve harm to the organisation. Deterrence can be generated based on the effectiveness, or perceived effectiveness of controls in other layers and may be sufficient to deter a would-be perpetrator from carrying out their intent. Where a

person is not deterred from committing the act, the Prevent layer is a collection of controls and functions which act to identify and monitor suspicious behaviour and then stop the risk event from taking place before the information is compromised. Both the Shape and Prevent layers are made up of three interlinked functions; Detect, Alert, and Respond. For one example in the Shape layer, these functions combine to detect potential insider vulnerability traits in job applicants, alert the interview panel, and a decision is made to not employ that applicant if they are above a predetermined threshold, reducing the risk to the organisation. For the Prevent layer, the three functions are needed to generate awareness of the perpetrators actions, raise an alert or alarm, undertake decision making and execute a responsive action to stop the risk event from taking place. Each layer alone, if fully effective, could potentially reduce the likelihood of a successful attack to zero.

Where a risk event is not stopped, and information has been compromised, there are still security controls which can be emplaced to reduce some of the consequences and impacts of the event. Post-event layers include Protect, Contain and Recover/Adapt. The Protect layer consists of passive, impact-specific controls such as encryption to deny access to information that is stolen, or in the physical domain, enforced standoff to protect high value buildings from vehicle-borne explosive devices. The Contain layer involves the same active functions as in Prevent or Shape, that is, Detect, Alert and Response, although the nature of these functions is quite different here, where it involves detecting the breach and raising actions that manage the harm, rather than actions to stop the breach occurring. The Recover/Adapt layer stops immediate consequences escalating to greater organisational impacts and is often encapsulated under principles of business continuity or resilience. As many insider attacks are an accumulation of multiple small attacks, the Investigate layer for such threats is vital as collection of data over time may help identify and stop future attacks based on those that were previously unresolved in the past.

3 SECURITY-IN-DEPTH FOR MANAGING INSIDER THREATS

In this section we intend to illustrate the utility/applicability of SiD to insider threat management. We do this by developing a semi-quantitative analysis of an example scenario to show the relative effectiveness of two different security enhancement approaches (strategies). We start from the premise that our ‘organisation’ has some (default) security in place, but it is considered deficient in managing insiders, as we see the impacts of the harm they generate. The “board” has agreed to invest in additional security and we are presented with two different philosophies for managing insiders. In our example they are deliberately rather stark – in reality these options would be much more balanced and holistic. The first (option A) focuses on cultural, procedural, educational and psychological controls while the second (option B) focuses on technologies that improve the monitoring, access, management and loss prevention of information.

The vignette we “play” is that of compromising confidentiality through exfiltration of sensitive information through three vectors:

- The careless insider – careless mishandling of digital media left in public place,
- The disloyal insider – deliberate removal and sale to a third party, and
- The mole – social engineering to gain access, and distribution to a foreign agency.

We therefore have three different insider scenarios playing out against three different security systems (the current default, option A and option B) which gives us nine combinations to evaluate. We represent the attack sequences or pathways for each insider type in Fig. 4. Each pathway begs interventions to break its progression, and the nature of

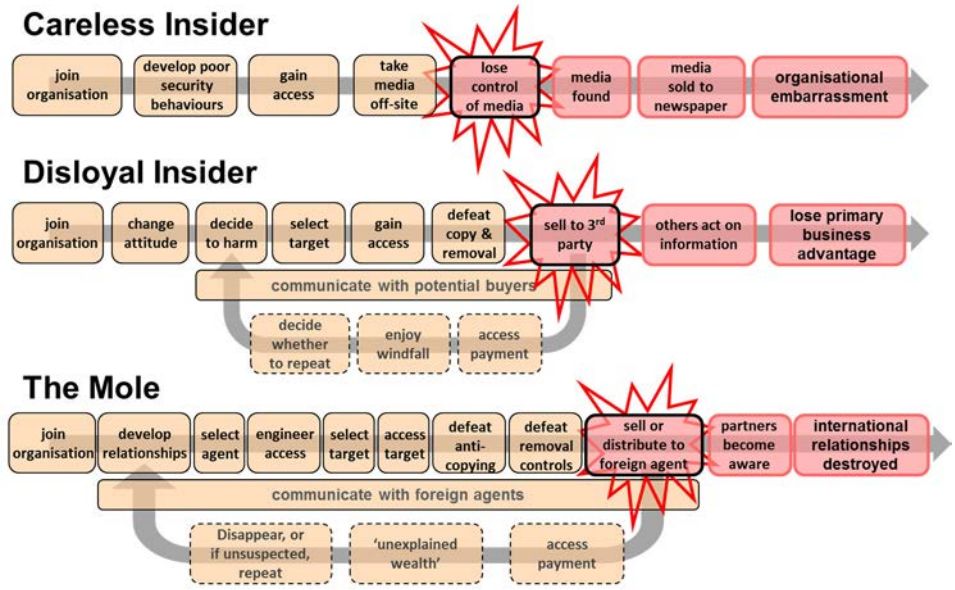

Figure 4: Different attack pathways for three types of insiders. The security breach is represented by the star element in each pathway.

those interventions is different for each pathway. For the disloyal insider and the mole, the pathways also include some return elements which provide additional opportunities to catch these perpetrators, possibly not during the first successful attack but from future attacks.

In applying the SiD framework, the method is to utilise the layers, and decide which layers are relevant as interventions along each pathway. Interventions that reduce the probability of the risk event occurring (Shape, Deter and Prevent) are useful before the breach (the star element in the pathways shown in Fig. 3). Consequence management layers (Protect, Contain and Recover/Adapt) are relevant for the post-breach elements as ways of managing impacts. To keep this example as simple as possible, we will consider a single risk event and not an insider repeating the same event multiple times. As the purpose of the Investigate layer of SiD is to collect evidence from previous attacks in order to stop future attacks, its contribution to risk reduction is excluded from this example.

Our evaluations require elicitation from experts, who estimate (based on which security system is under examination) the contribution of each layer to reducing the probability of the breach event occurring, or its consequences and impacts. Those probabilities and impacts will vary, depending on which security system is under consideration.

Table 1 is a representation of how such an analysis may be constructed. The table is divided into three main columns (the default security package, and the enhanced security solutions from investment in options A and B). Some example controls for each layer are also provided. The top half of the table shows our (hypothetical) experts' estimates of the numerical probability of the breach event occurring (through the individual and combined effects of Shape, Deter and Prevent layers).

The bottom half of the Table 1 considers the consequence/impact distributions (not enumerated) according to the effectiveness of Protect, Contain and Recover layers. There are many ways that consequences might be enumerated, for example, in monetary terms, in time

(as in a delay to market) or perhaps in damage terms such as lost output or even loss of lives. In Table 1, C is a random variable representing the consequence which can either be a discrete or a continuous random variable depending on how one decides to enumerate the consequences. For this example, we divide the space of consequences into (arbitrarily) three divisions, ie, 'low', 'medium' and 'high'. Our 'experts' are then asked to estimate the chances of low consequence, the chances of medium consequence etc, according to each scenario and security system, using a stochastic mapping approach as shown in Fig. 5.

Table 1: Example risk analysis process for comparing investment options A and B to improve the current (default) insider security system.

Layers	Default controls			Control options A			Control options B		
Shape	Background checks - Rejection								
	Probation – Termination			Human resource intelligence – Feel good programs					
Probability of insider developing motivation									
	Careless	Disloyal	Mole	Careless	Disloyal	Mole	Careless	Disloyal	Mole
	0.8	0.9	1.0	0.7	0.8	1.0	0.8	0.9	1.0
Deter	Visible security			Self-monitoring team			Misinformation		
	Annual security awareness courses								
Probability of motivated insider deciding to act									
	Careless	Disloyal	Mole	Careless	Disloyal	Mole	Careless	Disloyal	Mole
	0.7	0.8	1.0	0.5	0.6	1.0	0.7	0.8	0.9
Prevent	Network monitoring						Data loss prevention suite		
	Removable media detection/ restrictions						Honeypot		
Probability of successful attack when the plan is executed									
	Careless	Disloyal	Mole	Careless	Disloyal	Mole	Careless	Disloyal	Mole
	0.8	0.9	1.0	0.8	0.9	1.0	0.7	0.8	0.9
Probability of risk event occurring									
$P = \prod_{i=1}^{3} P_i$	Careless	Disloyal	Mole	Careless	Disloyal	Mole	Careless	Disloyal	Mole
	0.45	0.65	1.0	0.28	0.43	1.0	0.39	0.58	0.81

Layers	Default controls			Control options A			Control options B		
Protect	Least privilege access to data			Additional separation of duties to reduce access to data			Encryption		
Probability distribution of consequence after Protect controls									
	Careless	Disloyal	Mole	Careless	Disloyal	Mole	Careless	Disloyal	Mole
	C_1^x	C_2^x	C_3^x	C_4^x	C_5^x	C_6^x	C_7^x	C_8^x	C_9^x
Contain	Ransom payments			Recovery negotiation team			Alert beacons		
							Plant false information		
Probability distribution of consequence after Contain controls									
	Careless	Disloyal	Mole	Careless	Disloyal	Mole	Careless	Disloyal	Mole
	C_1^y	C_2^y	C_3^y	C_4^y	C_5^y	C_6^y	C_7^y	C_8^y	C_9^y
Recover	Continuity plan			Resilience workforce					
	Business agility								
Probability distribution of consequence after Recover controls									
	Careless	Disloyal	Mole	Careless	Disloyal	Mole	Careless	Disloyal	Mole
	C_1^z	C_2^z	C_3^z	C_4^z	C_5^z	C_6^z	C_7^z	C_8^z	C_9^z

	Default controls			Control options A			Control options B		
Probability distribution of risk (residual risk)									
$R = f(P, C)$	Careless	Disloyal	Mole	Careless	Disloyal	Mole	Careless	Disloyal	Mole
	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9

Security panel survey question: Given the implementation of controls through the Protect layer (denoted by the superscript x), what is the chance of (low, medium, high) level of immediate consequences arising from a risk event?

C_6^x

Threat: Mole	Security: Option A		
Consequence Scale	Low	Medium	High
Distribution (%)	0	30	70

Figure 5: Example of eliciting the consequence distributions for the three security layers that contribute to consequence reduction. Refer to bottom half of Table 1.

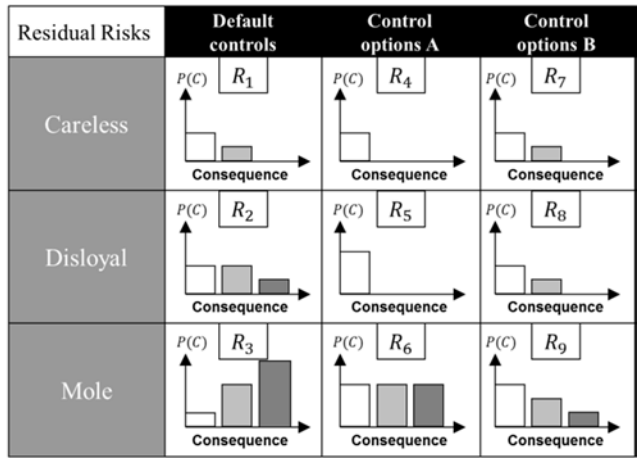

Figure 6: The residual risks for the three insider types under investigation with the default insider security system, and the addition of control options A and B.

By combining probabilities and consequences we arrive at the summary evaluation of the residual risk shown at the foot of Table 1 and in Fig. 6. At this point, decision makers are able to see the value of each security enhancement according to $R = f(P, C)$. We have used a simple three bin approach to make the outcomes visually obvious however in reality decision makers might prefer to use expected values, value at risk, or other more established measures.

We have deliberately engineered this hypothetical analysis to show that enhancement option A stochastically dominates option B, that is, it reduces risk more effectively for the careless and disloyal insiders, but option B does a better job in managing the high end impacts of a mole. Decision makers must decide, based on their particular organisation's threat profile, where it should invest including, of course, other considerations such as capital, training and ongoing maintenance costs etc. Refer to [44] for more details of this step.

4 CONCLUSION

Insiders are an ever-present threat to organisations with the potential to cause significant financial and reputational damage. The spectrum of insiders from careless to implanted mole necessitates a variety of controls to manage the combined risk from insiders to the organisation. The literature on insider threats provides security managers with detailed lists

of possible controls to implement, insider threat pathways to identify opportunities to control the insiders, and strategies for where priority should be placed. However, it is still difficult for the security manager to determine what sets of controls to implement to achieve the greatest benefit-cost for their security investment.

We address this gap in the literature through the use of a risk-based framework called Security-in-Depth. The framework's construct of explicitly defined and independent layers allows decision makers to (1) assess the performance of integrated sets of controls at reducing insider risk (through reducing the likelihood of a breach or reducing the consequences when a breach does occur), and (2) prioritise security investment solutions to maximise benefit-cost. We have applied the framework to a hypothetical insider problem to demonstrate its utility to support investment decisions by the security manager. The worked example, which was not intended to characterise real properties of insider threat profiles, demonstrated how different security enhancement strategies have differing effectiveness on the three kinds of insiders we used in this example. The security manager applying this process (and adapting the approach to their circumstances) would be able to decide which strategy generates greater benefit-cost. This framework has been applied and valued by decision makers in other related security contexts.

REFERENCES

[1] *CERT Common Sense Guide to Mitigating Insider Threats*, 5th ed., 2016.
[2] *CERT 2011 Cybersecurity Watch Survey. How Bad is the Insider Threat?* 2011.
[3] Hua, J. & Bapna, S., Who can we trust?: the economic impact of insider threats. *Journal of Global Information Technology Management*, **16**(4), pp. 47–67, 2013. DOI: 10.1080/1097198X.2013.10845648.
[4] Upton, D.M. & Creese, S., The danger from within. *Harvard Business Review*, pp. 95–101, Sep. 2014.
[5] Wang, Y.L. & Yang, S.C., A method of evaluation for insider threat. *Proceedings of the 2014 International Symposium on Computer, Consumer and Control*, pp. 438–441, 2014. DOI: 10.1109/IS3C.2014.121.
[6] Reidy, P. & Randal, K., Combating the insider threat at the FBI: real world lessons learned. Presented at *RSA Conference*, San Francisco CA, 2013.
[7] Greene, R., Kehl, D., Morgus, R. & Bankston, K., *Surveillance Costs: the NSA's Impact on the Economy, Internet Freedom and Cybersecurity*, 2014.
[8] Ophoff, J., Jensen, A., Sanderson-Smith, J., Porter, M. & Johnston, K., A descriptive literature review and classification of insider threat research. *Proceedings of Informing Science & IT Education Conference*, pp. 211–223, 2014.
[9] Zeadally, S., Yu, B., Jeong, D.H. & Liang, L., Detecting insider threats: solutions and trends. *Information Security Journal: A Global Perspective*, **21**(4), pp. 183–192, 2012. DOI: 10.1080/19393555.2011.654318.
[10] Guido, M.D. & Brooks, M.W., Insider threat program best practices. *Proceedings of the 46th Annual Hawaii International Conference on System Sciences*, pp. 1831–1839, 2013. DOI: 10.1109/HICSS.2013.279.
[11] Ahmad, A., Maynard, S.B. & Park, S., Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, **25**(2), pp. 357–370, 2014. DOI: 10.1007/s10845-012-0683-0.
[12] US Department of Homeland Security, Combating the insider threat, National Cybersecurity and Communications Integration Center, 2014.
[13] Smith, J.A., *Mitigating Malicious Insider Cyber Threat*, Royal Holloway University of London, UK, 2015.

[14] Sanzgiri, A. & Dasgupta, D., Classification of insider threat detection techniques. *Proceedings of the 11th Annual Cyber and Information Security Research Conference*, 2016. DOI: 10.1145/2897795.2897799.
[15] Hunker, J. & Probst, C.W., Insiders and insider threats: an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, **2**(1), pp. 4–27, 2011. DOI: 10.22667/JOWUA.2011.03.31.004.
[16] Hashem, Y., Takabi, H., GhasemiGol, M. & Dantu, R., Inside the mind of the insider: towards insider threat detection using psychophysiological signals. *Journal of Internet Services and Information Security*, **6**(1), pp. 20–36, 2016. DOI: 10.22667/JISIS.2016.02.31.020.
[17] Almehmadi, A. & El-Khatib, K., On the possibility of insider threat prevention using intent-based access control (IBAC). *IEEE Systems Journal*, **11**(2), pp. 373–384, 2017. DOI: 10.1109/JSYST.2015.2424677.
[18] Securelist. Recognizing Different Types of Insiders. https://securelist.com/threats/recognizing-different-types-of-insiders/. Accessed on: 14 Oct. 2011.
[19] Greitzer, F.L. et al., Developing an ontology for individual and organizational sociotechnical indicators of insider threat risk. *Proceedings of the 11th International Conference on Semantic Technology for Intelligence, Defense, and Security*, pp. 19–27, 2016.
[20] Bishop, M. et al., A risk management approach to the 'insider threat'. *Insider Threats in Cyber Security*, eds C.W. Probst, J. Hunker, M. Bishop & D. Gollmann, Springer: New York, NY, pp. 115–137, 2010. DOI: 10.1007/978-1-4419-7133-3.
[21] IAEA Preventive and protective measures against insider threats, International Atomic Energy Agency, Vienna, Austria, 2008.
[22] Duran, F.A., Conrad, S.H., Conrad, G.N., Duggan, D.P. & Held, E.B., Building a system for insider security. *IEEE Security & Privacy*, **7**(6), pp. 30–38, 2009. DOI: 10.1109/MSP.2009.111.
[23] Nurse, J.R.C. et al., Understanding insider threat: a framework for characterising attacks. *Proceedings of the IEEE Security and Privacy Workshops*, pp. 214–228, 2014. DOI: 10.1109/SPW.2014.38.
[24] Kammuller, F., Nurse, J.R.C. & Probst, C.W., Attack tree analysis for insider threats on the IoT using Isabelle. *Proceedings of the 4th International Conference on Human Aspects of Security, Privacy and Trust*, 2016.
[25] Musman, S. & Turner, A.J., A game-oriented approach to minimizing cybersecurity risk. *International Journal of Safety & Security Engineering*, **8**(2), pp. 212–222, 2018. DOI: 10.2495/SAFE-V8-N2-212-222.
[26] Maybury, M. et al., Analysis and detection of malicious insiders. *Proceedings of the International Conference on Intelligence Analysis*, 2005.
[27] Cole, E. & Ring, S., *Insider threat: protecting the enterprise from sabotage, spying, and theft*, Syngress: Rockland MA, 2006.
[28] Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E., The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, **24**(6), pp. 472–484, 2005. DOI: 10.1016/j.cose.2005.05.002.
[29] Wang, H., Xu, H., Lu, B. & Shen, Z., Research on security architecture for defending insider threat. *Proceedings of the 5th International Conference on Information Assurance and Security*, pp. 30–33, 2009. DOI: 10.1109/IAS.2009.53.
[30] Catrantzos, N., Tackling the insider threat, ASIS International Foundation CRISP Report, 2010.

[31] Montelibano, J. & Moore, A., Insider threat security reference architecture. *Proceedings of the 45th Annual Hawaii International Conference on System Sciences*, pp. 2412–2421, 2012. DOI: 10.1109/HICSS.2012.327.
[32] Park, S., Ruighaver, A.B., Maynard, S.B. & Ahmad, A., Towards understanding deterrence: information security manager's perspective. *Proceedings of the International Conference on IT Convergence and Security*, pp. 21–37, 2012. DOI: 10.1007/978-94-007-2911-7_3.
[33] Australian Government, *Managing the Insider Threat to Your Business: a Personnel Security Handbook*, 2016.
[34] Buckley, O., Nurse, J.R.C., Legg, P.A., Goldsmith, M. & Creese, S., Reflecting on the ability of enterprise security policy to address accidental insider threat. *Proceedings of the Workshop on Socio-Technical Aspects in Security and Trust*, pp. 8–15, 2014. DOI: 10.1109/STAST.2014.10.
[35] Stavrou, V., Kandias, M., Karoulas, G. & Gritzalis, D., Business process modeling for insider threat monitoring and handling. *Trust, Privacy, and Security in Digital Business*, eds C. Eckert, S.K. Katsikas & G. Pernul, Springer, pp. 119–131, 2014. DOI: 10.1007/978-3-319-09770-1_11.
[36] Forcht, K.A., *Computer Security Management*, Boyd & Fraser: Danvers, MA, 1994.
[37] Straub, D.W. & Welke, R.J., Coping with systems risk: security planning models for management decision making. *Management Information Systems Quarterly*, **22**(4), pp. 441–469, 1998.
[38] Stolfo, S., Bellovin, S.M. & Evans, D., Measuring security. *IEEE Security & Privacy*, **9**(3), pp. 60–65, 2011. DOI: 10.1109/MSP.2011.56.
[39] Pan, L. & Tomlinson, A., A systematic review of information security risk assessment. *International Journal of Safety & Security Engineering*, **6**(2), pp. 270–281, 2016. DOI: 10.2495/SAFE-V6-N2-270-281.
[40] Nunes-Vaz, R., Lord, S. & Ciuk, J., A more rigorous framework for security-in-depth. *Journal of Applied Security Research*, **6**(3), pp. 372–393, 2011. DOI: 10.1080/19361610.2011.580283.
[41] Lord, S. & Nunes-Vaz, R., Designing and evaluating layered security. *International Journal of Risk Assessment and Management*, **17**(1), pp. 19–45, 2013. DOI: 10.1504/IJRAM.2013.054377.
[42] Nunes-Vaz, R. & Lord, S., Designing physical security for complex infrastructures. *International Journal of Critical Infrastructure Protection*, **7**(3), pp. 178–192, 2014. DOI: 10.1016/j.ijcip.2014.06.003.
[43] Nunes-Vaz, R., Lord, S. & Bilusich, D., From strategic security risks to national capability priorities. *Security Challenges*, **10**(3), pp. 23–49, 2014.
[44] Rowe, C. et al., Prioritizing investment in military cyber capability using risk analysis. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, pp. 1–13, 2017. DOI: 10.1177/1548512917707077.