System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis

Tesleem Fagade[1], Theo Spyridopoulos[2], Nabeel Albishry[1], and Theo Tryfonas[1](✉)

[1] Cryptography Group, University of Bristol, Bristol, UK
{tesleem.fagade,n.albishry,theo.tryfonas}@bristol.ac.uk
[2] Cybersecurity Research Unit, University of the West of England, Bristol, UK
theo.spyridopoulos@uwe.ac.uk

Abstract. Enforcing cybersecurity controls against malicious insiders touches upon complex issues like people, process and technology. In large and complex systems, addressing the problem of insider cyber threat involves diverse solutions like compliance, technical and procedural controls. This work applies system dynamics modelling to understand the interrelationships between three distinct indicators of a malicious insider, in order to determine the possibility of a security breach through developing trends and patterns. It combines observable behaviour of actors based on the well-established theory of planned behaviour; technical footprints from incident log information and social network profiling of personality traits, based on the 'big five' personality model. Finally, it demonstrates how system dynamics as a risk modelling approach can flag early signs of malicious insider threats by aggregating associative properties of different risk elements. Our initial findings suggest that key challenges to combating insider threats are uncertainty, irregular intervals between malicious activities and exclusion of different personality factors in the design of cyber-security protocols. Based on these insights we propose how this knowledge may help with mitigation controls in a secure environment.

Keywords: Malicious insider · Cyber security · Risk modelling · System dynamics · Cyber-risk behaviour · Personality profiling

1 Introduction

An organization's continual effort to reinforce its cyber capabilities and the unique challenge posed by malicious insiders, borders on complex issues that encompass different loosely coupled variables; people, process and technology. Even more so, constructing tools to address this issue often involves diverse controls like technical, procedural, formal and informal solutions, which are difficult to apply in large and complex systems [4]. Organizations' growing reliance on large-scale interconnected information assets and widely available sophisticated attacker tools, suggest that the prevalence and impact of cyber-attacks is set for rapid increase [5]. Insider problem is widely documented in security reports, based on the U.S Secret Service and Verizon reports, of confirmed security breach cases in 2009 alone, insiders are responsible for

T. Tryfonas (Ed.): HAS 2017, LNCS 10292, pp. 309–321, 2017.
DOI: 10.1007/978-3-319-58460-7_21

46% of data breaches, of which 90% were malicious and deliberate acts [3]. Trusted users' elevated access to information utility is a major concern when addressing the problems of insider threat, given that these users already sits behind organizations firewall. Many literature agrees that insiders are the weakest link in organizations defence posture [6, 7], and that insiders are responsible for system exploits more than the failure of technical and procedural measures.

Insider threat manifests when agents' behaviour is contrary to regulatory policies and guidelines. It refers to harmful acts that a trusted employee may carry out to undermine the confidentiality, integrity and availability of information assets. Currently, there is no complete, effective and systemic method developed to address cyber security challenges. The number of attempts to address human factors in cyber security is quite low despite evidence suggesting that a malicious insider exhibits in advance of exploit, an observable 'concerning behaviour' [3]. While the importance of security deterrence investment cannot be completely discounted, the effectiveness against malicious insider is questionable. Deterrence measures can be applied in many ways; for instance, by integrating reward and punishment elements into organisation policies and procedures in order to discourage, remind or compel employees into secure behaviour. However, policies and procedures are behaviour oriented and there is no absolute certainty that people always do as told. What are the key drivers of malicious acts? Are they preventable? It has been shown that security by compliance, as a way to address insider threat problems is a farfetched approach [2], therefore, addressing malicious insider cyber-threat requires a more dynamic approach for analyzing patterns as a precursor to threat.

This work applies system dynamics modelling to understand the interrelationship between three distinct indicators of malicious insider activities. Risk indicators from different domains are aggregated in order to predict the possibility of a security breach, based on how the indicators influence one another. System Dynamics can be used to link hypothesized structure with observed behaviour of systems over a period of time, thereby allowing feedback to uncover certain types of endogenous phenomena [10]. This work combines a behavioural and psychological model of planned behaviour theory; observable personality profiling of actors through social network footprints and system audit trails established from IT resource incident log information. Finally, it demonstrates how system dynamics can flag early signs of malicious insider problems, based on the associative properties of different risk elements. Motivation for this work and relevant literature is covered in Sect. 2. Overview of modelling of the interconnected risk domains is presented in Sect. 3. Methodology and simulation environment including model assumptions is presented in Sect. 4, while Sect. 5 covers discussion and future work.

2 Related Work and Motivation

We review some of the research done in attempt to model insiders' threat behaviour in organisations, but this is by no means an exhaustive list. In terms of understanding the primary driver for malicious behaviour, some of the work in this area [31–36] use decision algorithms to assess the predisposition to malicious behaviour by combining psychometric test scores data and real time technical data obtained from users' information systems. Another literature describes malicious insider threats through a devised taxonomy of attributes; access, risk, knowledge, process and motivation, in order to analyze how each or a combination of these attributes stimulate malicious insiders' behaviour [11]. [9] applies Bayesian network model to study the motivation and psychology of malicious insiders, while [1] evaluates the probability of insider threat detection through a conceptual model that connects real world measurements and a hypothesis-tree, and [28] describes how technical assessment can be combined with information assets categorization and agents behaviour in order to mitigate insider-threat problems through resilience, survivability and security.

In addition, research also shows that employees do not just carry out malicious acts randomly but show some signs of malicious behaviour well in advance of cyber-attacks. In this light, some work emphasize the importance of recognizing early signs of risky behaviour. For instance, [3], described a predictive modelling framework for automated support and detection of high-risk behavioural indicators that may help form risk mitigating decisions. Other research emphasizes the link between personality traits and the tendency to become a malicious insider. Importantly, it is suggested that people's personality can be revealed through the online social media platforms like the Facebook, Twitter and YouTube posts, from which personality types can be mapped to specific job roles, in order to mitigate insider threats [24, 29]. In particular, [32] reveals how it is possible to harvest publicly available information from YouTube video comments, that may identify personality traits through combined dictionary based text classification and machine learning techniques. Similarly, [14] suggests that the personality trait of narcissism is a common characteristics of malicious insiders and that information shared in public domain like Twitter can be utilized to establish predictive actions and deterrence measures against malicious insiders.

It is clear from the relevant literature that detecting insider activities requires more than a single indicator. [19, 27] recommends that there is a need for a framework that encompasses multiple risk indicators for a holistic and predictive threat detection. This paper furthers our previous work on insiders' problem by developing a System Dynamics Model for early detection of insider threat activities, based on personality, behavioural and technical risk indicators. It particularly focuses on malicious insider actions, given that privileged access abuse by malevolent insiders is hard to lock down.

3 Overview of Model Interconnected Risk Domains

For the purpose of this work, we model malicious insider problems by taking into account personality, behavioural and technical risk indicators. Simulating multiple indicators of risk, based on the activities of an employee illustrates a broader implication for collective management of information security. Insider threat detection requires proactive analysis of multiple trigger factors far beyond network analysis alone. Hence, the idea of interconnected domains approach is based on the notion that different elements of risks are inextricably linked, therefore making each contributing factor a function of the malicious insider problem.

3.1 Personality Risk Indicators

Although a personality trait is fairly stable through individuals' lifetimes, the ability to establish a statistically significant relationship between various personality profiles can provide guidelines for implementing security protocols that meet individual needs in a diverse workforce [8]. There are different ways of assessing personality types based on the five psychological construct of Openness, Conscientiousness, Extroversion, Agreeableness and Narcissism (OCEAN). Using publicly available information on Twitter alone, it is possible to predict personality trait to within 11% [23], because certain words tend to be used repeatedly, leading to a pattern that can be correlated with a specific personality trait. Also, through category based textual analysis of browsing behaviour and webpage content, LIWC (Linguistic Inquiry and Word Count) dictionary can be applied to group and link linguistic terms with personality traits [25]; such that, each element of the OCEAN construct can be directly linked to specific malicious activities.

Employees do not only transfer offline behaviour to online social network platforms, there are also evidence to suggest a connection between excessive use of social media and narcissist personality trait [15–17]. Self-promoting contents combined with high level of online activities are also strongly correlated with low self-esteem, malevolent system use, narcissist personality and delinquent behaviour [18]. Personality trait of Openness is linked with susceptibility to phishing, while narcissism, agreeableness and excitement seeking is linked with insider threat and antisocial behaviour [25, 34]. People also reveal certain attributes through social media platforms, relating to psychosocial states like anxiety, debt, adjustment disorder and medical conditions, from which psychosocial risk factors could be drawn.

Although, personality is a direct determinant of intention, individuals with different personality traits are more likely to react differently to the same security scenario, threats and organisation sanctions based on their perception of deterrence, protection motivation or efficacy factors [8]. Consider the generic personality model shown in Figs. 1 and 2,

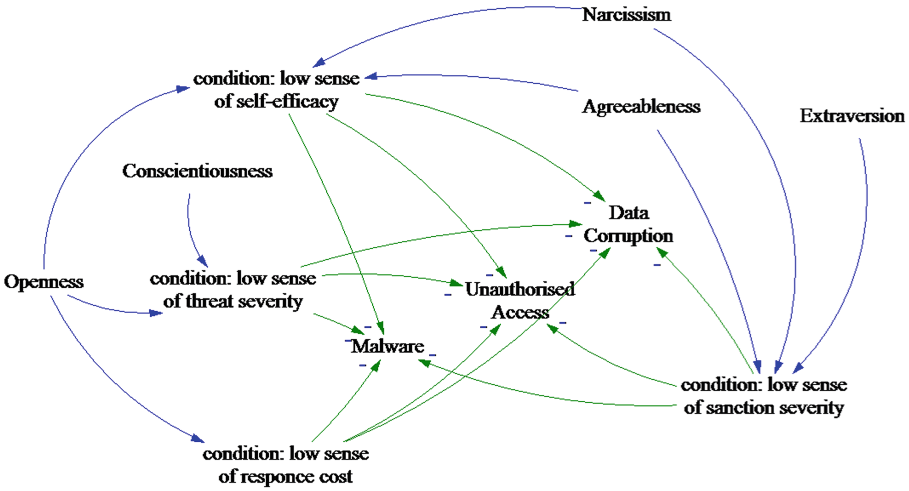
Narcissism
condition: low sense of self-efficacy
Agreeableness
Extraversion
Conscientiousness
Data Corruption
Openness
condition: low sense of threat severity
Unauthorised Access
Malware
condition: low sense of sanction severity
condition: low sense of responce cost
-

Fig. 1. Cybersecurity risk reduces due to personality traits under specified conditions

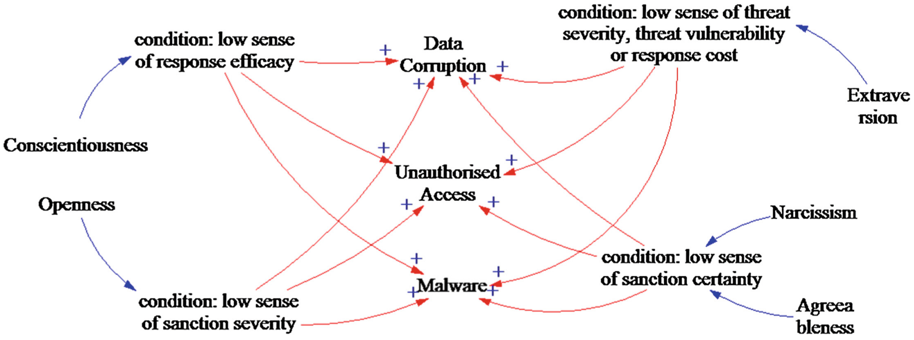
condition: low sense of response efficacy
Data Corruption
condition: low sense of threat severity, threat vulnerability or response cost
Extraversion
Conscientiousness
Unauthorised Access
Openness
Narcissism
condition: low sense of sanction certainty
Malware
condition: low sense of sanction severity
Agreeableness
+

Fig. 2. Cybersecurity risk increases due to personality traits under specified conditions

adopted from [8], it can be seen that an individual with 'Extraversion' personality trait, but with a low sense of sanction severity, is less likely to violate cyber security protocols than an individual with 'Openness' personality trait and low sense of sanction severity. Likewise, an individual with 'Extraversion' personality but with low sense of threat severity, threat vulnerability or response cost is more likely to violate security protocols than an individual with 'Conscientiousness' personality trait with low sense of threat severity or someone with 'Openness' personality trait with low sense of response cost.

3.2 Behavioural Risk Indicators

Theory of planned behaviour has its foundation on a number of constructs and it helps us to understand the reason for deliberate behaviour. It explains why it is hard to change how malevolent insider perceives security protocols. Security managers may provide training, policies and guidelines but users do not necessarily comply, even when mandated. Important aspect of the theory of planned behaviour is that, given a degree of control over events, people are expected to carry out their behaviour, however, intentions can change on the emergence of new information [13]. Previous behaviour and actions of malevolent user can help inform future actions but the challenge is that behaviour may not be easily quantifiable, if there is irregular intervals between malicious activities or no prior established patterns.

Behavioural theories provide guidelines on how behaviour may manifest in different stages of an insider threat scenario through certain indicators. The theory of planned behaviour suggests that a person's intention, perceived behaviour towards crime, subjective norms and attitude are key factors in predicting behaviour [20]. Pre-employment background checks, 360 profiler and other mechanism may help to identify agents that constitute behavioural risk, some of which may be unrelated to employment, like anxiety, breakup, depression, debt and medical conditions [26]. Though some risks may not directly link psychological behaviour to criminal background but may help address psychological factors required to form group homogeneity [12, 14]. Based on 23 cases of insider threat in the banking and finance sector, 33% is due to personal problems that are unrelated to employment, like breakup and anxiety;

23% is due to revenge, 27% is due to debt and 81% is due to financial gains [21]. In another report [22], based on a case study of 52 illicit cyber activities in the IT and Telecommunication sector; 33% is due intolerant to criticism, 57% involves disgruntled employees, 47% is revealed through overt behaviour, and 58% involves direct communication of threat online.

Behaviour and external environmental influences can indicate early signs of cyber-security risks, as shown on the generic system dynamic diagram in Fig. 2. The more an individual exhibits one or more combinations of the behavioural risk elements, the more likely it is to violate cyber security protocols. Human resource staff are particularly well trained to apply observation techniques, recognize and report high scoring risk indicators as a predictor of anomalous behaviour.

3.3 Technical Risk Indicators

There are six categories of critical log information that can be used to identify suspicious activities. These include authentication, system and data change, network activity, resource access, malware activity, failure and critical error logs. Security tools like SIEM/log analysis, data access monitoring, intrusion detection/prevention systems (IDS/IPS) can be leveraged to provide administrators with sufficient information on suspicious activities [30]. Changes to configuration file binaries, network assets authentication and authorization log reports can be tracked to monitor employee activities. For instance, different patterns of system usage based on defined attributes can be combined with log information, job roles and privileges to create a profile for a normal user in a particular role. If there is an irregular pattern in the log information for a particular user compared to the activity of a normal user for the same role, then, that

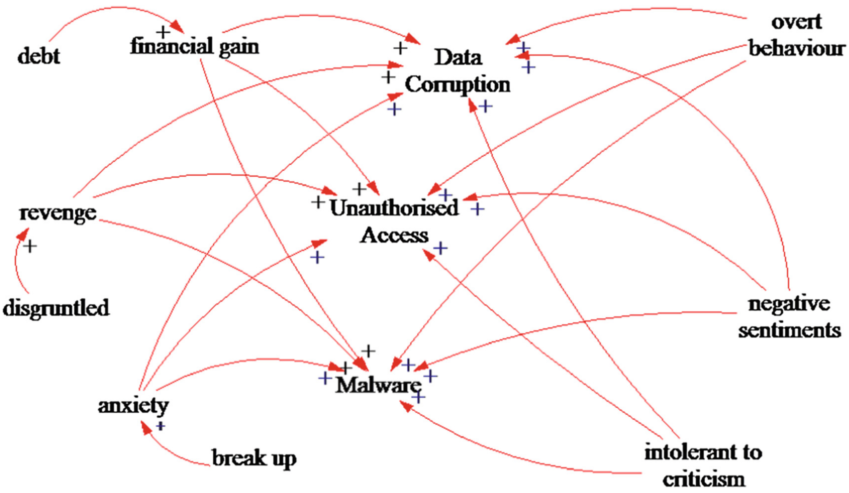

Fig. 3. Cybersecurity risk increases due to individual's behaviour or external influence with negative psychological effects

may suggest potential insider activities. Case study of 52 cyber incidents [22] shows that 57% of incidents are detected through system irregularities; of which 73% involves remote access logs and 57% involves unauthorized file access logs. Based on another study [33] involving 36 illicit cyber activity in the government sector, 24% of incidents is due to unauthorized privilege users and 11% involves installation of backdoors. Figures 2 and 3 shows how technical risk may be influenced by the interplay of other variables like personality traits and behaviour.

4 Methodology and Simulation Environment

4.1 Model Analysis

System Dynamics can be used to link hypothesized structure with observed behaviour of systems over a period of time, thereby allowing feedback to uncover certain types of endogenous phenomena [10]. Ventana Systems (Vensim PLE), a fully functional system dynamics software package, is used to conduct the simulation in this work. We propose that behavioural, technical or personality risk, when considered in isolation is not indicative of the full potentials of malicious insider. Irregular intervals between illicit cyber activities or inconsistent overt behaviour is difficult to apply independently as evidence of malicious insider. In order to prevent false positive triggers, each element of the risk indicators can be inextricably linked and modelled in order to draw more valid inferences. When risk factors are combined and observed as they change over a period of time, developing patterns can provide significant confidence in identifying potential malicious insider.

Consider the high level abstractions for the conceptual model shown in Fig. 4. Organisations can define an employee’s ‘normal’ security profile based on different risk indicators, deterrence, protection motivation, efficacy factors and job roles. Employee activities are then monitored over a period of time e.g. monthly, based on combined data flow from three domain streams. Social network data can be leveraged to determine personality trait for a particular employee. This could be a contentious issue, however we suggest that data from open social networks such as Twitter may be used legitimately and are made available by employees themselves. Human resource (HR) data provides input from constant monitoring and analyzing behavioural risk indicators for that employee, in addition to the employee’s psychological state (PS). Monitoring psychosocial behaviour is important because it could be exacerbated by external factors that are not necessarily related to an employee’s job. Likewise, incident log data obtained from the IT department is used to determine technical risk indicators. In order to determine the security status for an employee, inputs from external environment that forms PS are combined with behavioural risk factors from HR. Output from this can be influenced by the personality of a user. Then, depending on the personality of an employee and the employee’s perception of deterrence, protection motivation and efficacy factors, the likelihood of cyber-security protocol violation can be determined. For instance, someone with ‘Narcissistic’ personality and low sense of sanction certainty is more likely to cause cyber leakage, espionage or delete system critical files, if associated PS and HR variables are true. Similarly, someone with

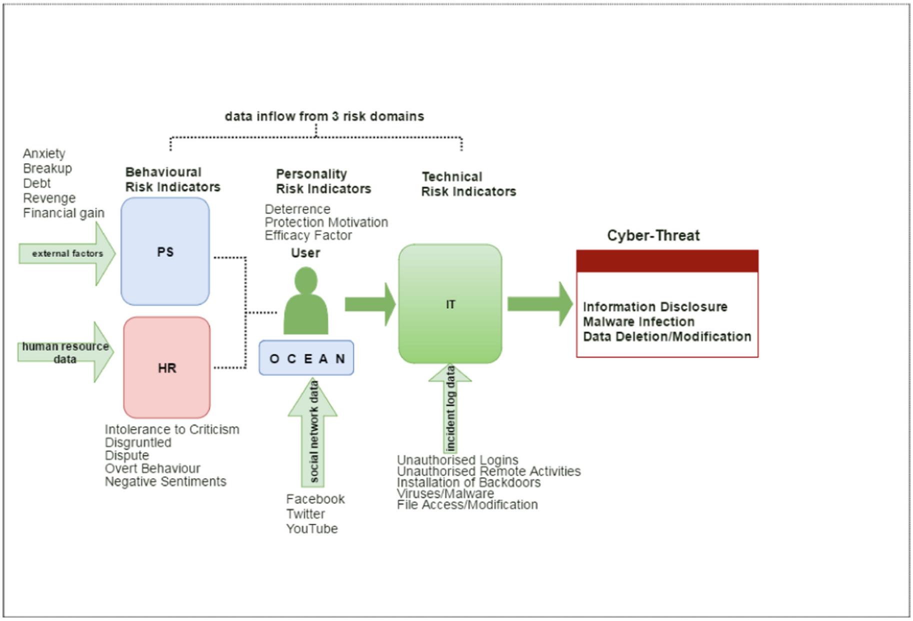

Fig. 4. High level abstraction of our insider threat modelling process

'Agreeable' personality with low sense of sanction certainty is more likely to be susceptible to phishing, if associated PS and HR factors are triggered.

4.2 Model Results and Discussion

The dynamic relationship diagram in Fig. 5 presents the stocks and flows that describes the dynamics between a person's behaviour, personality and the probability of a cyber-security incident (data corruption or unauthorized access), based on the generic system dynamics diagrams provided in Figs. 1, 2 and 3. In particular, we consider behaviour as the combination of a person's psychosocial state (PS), sculptured by external triggers (e.g. breakup or debt), with employee's internal behaviour (e.g. intolerance to criticism or negative sentiments) as observed by the HR department. Negative internal behaviour combined with an unhealthy psychosocial state can increase the probability of a cyber-security incident. On the other hand, personality can play a twofold role; as shown in our generic model (Figs. 1, 2 and 3) depending on specific conditions (e.g. low sense of sanction severity or low sense of response cost) certain personality traits can either increase or decrease the probability of a cyber-security incident. To simplify our stocks and flows diagram we made the assumption that for the employee under consideration, apply the following conditions: "low sense of self-efficacy" and "low sense of threat severity". Under these assumptions and according to our generic diagrams, 'Extraversion' increases the probability of a cyber-security incident while 'Openness', 'Conscientiousness', 'Narcissism' and

‘Agreeableness’ decreases it. These relationships are captured in Fig. 5, where all personality traits except ‘Extraversion’ contribute to the decrease of the cyber-security incident risk. All variables in Fig. 5 take values from 0 to 1.

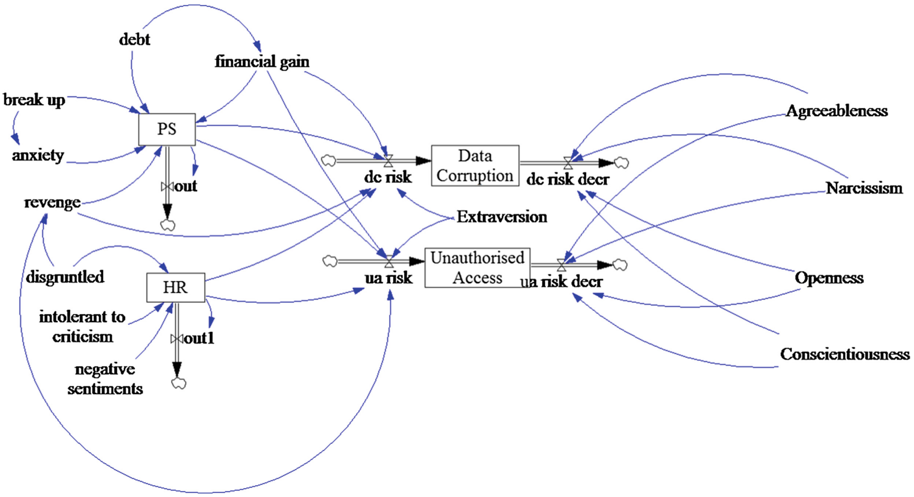

Fig. 5. Dynamic relationship between personality, behaviour and cyber-security incident

Figure 6 shows probability of data corruption in time for different combinations. Before we start the experiment, we set all personality traits to 1 and all internal behaviour and external psychosocial variables to 0. Then we change the following variables:

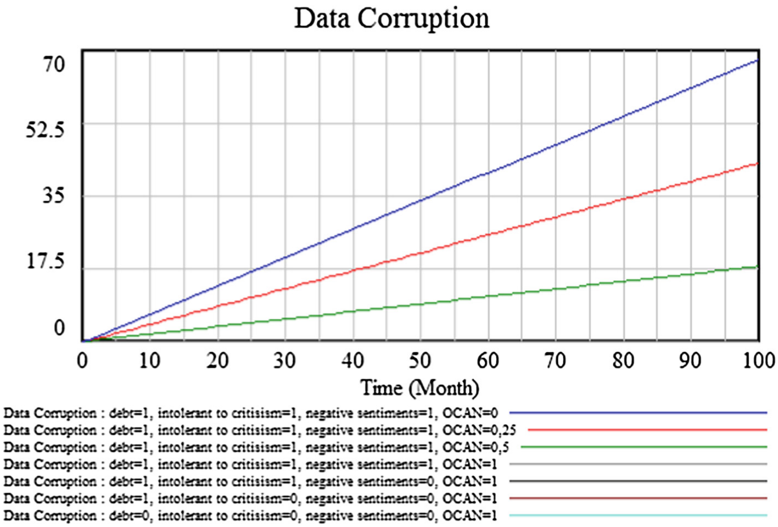

Fig. 6. Probability of data corruption in time based on personality

debt, intolerance to criticism, negative sentiments and O.C.A.N. (Openness, Conscientiousness, Agreeableness and Narcissism) and run the model for various combinations, as shown. As seen, personality plays an important role to cyber-security; the more open, conscientious, agreeable and not narcissist someone is, and depending on the associated deterrence, protection motivation and efficacy factors, the less likely it is to be involved in a cyber-security incident. However, as shown in Fig. 7, keeping constant the personality traits may still result in different cyber-security risk levels caused by the effect of external inputs (in this case debt) on the employee's psychosocial state. All experiments were made taking into account a particular set of conditions described in [8]. By changing these conditions and according to the description of our generic diagrams in Figs. 1, 2 and 3; changes in the personality would have different outcomes than the ones presented in Figs. 5 and 6.

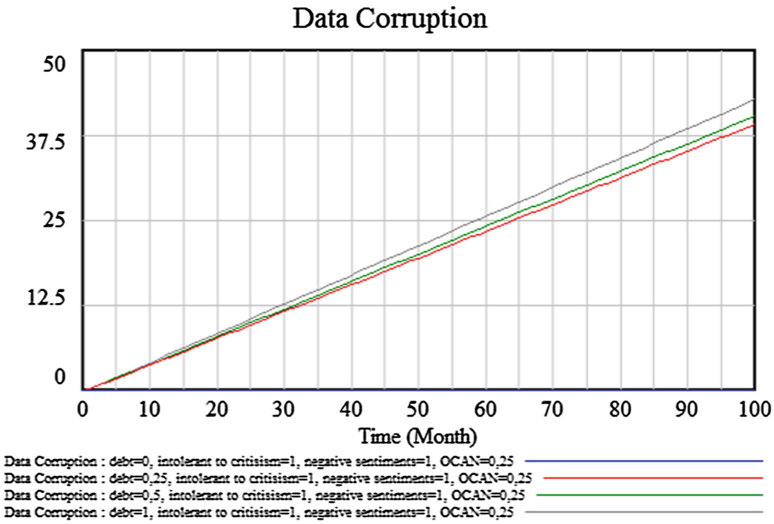

Fig. 7. Probability of data corruption in time based on behaviour

5 Conclusion and Future Work

This work describes a continuous feedback process for the detection of malicious insider cyber-threats, based on a system dynamics approach. There is an understandable limitation to the application of technical measures in order to mitigate malicious insider threats. Organisations should focus on a holistic response that integrate human factors with technical and procedural cyber capabilities. We seek to gain a rigorous understanding of how the interplay between individual personality traits, inherent behaviour and external influences is directly linked to the violation of cyber-security protocols. We have shown that, although personality traits differ between insiders, the motivation to violate or protect security protocols also varies in insiders with the same personality traits. Having the personality trait of one of the OCEAN elements does not make an individual more or less likely to violate a security protocol, but the perception of sanctions, rewards, psychological states and behaviour contributes to the likelihood of acting maliciously.

This study concludes that through combined behavioural analysis (HR) and externally triggered psychological factors (PS), technical footprints (IT) and personality types (OCEAN), the design and implementation of appropriate cyber-security protocols, should be based on a full understanding of insider psychological and security profiles. Providing generic cyber-security training and awareness programs without a deep understanding of employees outlook on deterrence, protection motivation or efficacy factors is simply a one-cap-fits-all approach that rarely ensures compliance. However, by customizing training based on individual personality traits and how they react to deterrence measures, organisation sanctions, threats, motivation and rewards; more positive results can be achieved. This observation is in line with earlier, more practical studies [37]. Based on these findings and a part of future research, we plan to develop a framework for customized cyber-security training that can appeal to different personality types.

References

1. Legg, P.A., et al.: Towards a conceptual model and reasoning structure for insider threat detection. JoWUA **4**(4), 20–37 (2013)
2. Fagade, T., Tryfonas, T.: Security by compliance? A study of insider threat implications for nigerian banks. In: Tryfonas, T. (ed.) HAS 2016. LNCS, vol. 9750, pp. 128–139. Springer, Cham (2016). doi:10.1007/978-3-319-39381-0_12
3. Greitzer, F.L., Hohimer, R.E.: Modeling human behavior to anticipate insider attacks. J. Strateg. Secur. **4**(2), 25 (2011)
4. Dhillon, G.: Violation of safeguards by trusted personnel and understanding related information security concerns. Comput. Secur. **20**(2), 165–172 (2001)
5. Andersen, D.F., et al.: Preliminary system dynamics maps of the insider cyber-threat problem. In: Proceedings of the 22nd International Conference of the System Dynamics Society (2004)
6. Corriss, L.: Information security governance: integrating security into the organizational culture. In: Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, Austin, Texas, USA, pp. 35–41. ACM (2010)
7. Aurigemma, S., Panko, R.: A composite framework for behavioral compliance within formation security policies. In: Proceedings of the 2012 45th Hawaii International Conference on System Sciences, pp. 3248–3257. IEEE Computer Society (2012)
8. McBride, M., Carter L., Warkentin, M.: Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. Technical report, RTI International (2012)
9. Axelrad, E.T., et al.: A Bayesian network model for predicting insider threats. In: 2013 IEEE Security and Privacy Workshops (SPW). IEEE (2013)
10. Martinez-Moyano, I.J., et al.: A behavioral theory of insider-threat risks: a system dynamics approach. ACM Trans. Model. Comput. Simul. (TOMACS) **18**(2), 7 (2008)
11. Wood, B.: An insider threat model for adversary simulation. SRI Int. Res. Mitig. Insider Threat Inf. Syst. **2**, 1–3 (2000)

12. Greitzer, F.L., Frincke, D.A.: Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In: Probst, C.W., Hunker, J., Gollmann, D., Bishop, M. (eds.) Insider Threats in Cyber Security. Springer, US (2010). 85–113
13. Ajzen, I.: From intentions to actions: a theory of planned behavior. In: Kuhl, J., Beckmann, J. (eds.) Action Control. Springer, Berlin (1985). 11–39
14. Kandias, M., Galbogini, K., Mitrou, L., Gritzalis, D.: Insiders trapped in the mirror reveal themselves in social media. In: Lopez, J., Huang, X., Sandhu, R. (eds.) NSS 2013. LNCS, vol. 7873, pp. 220–235. Springer, Heidelberg (2013). doi:10.1007/978-3-642-38631-2_17
15. Mehdizadeh, S.: Self-presentation 2.0: narcissism and self-esteem on Facebook. Cyberpsychol. Behav. Soc. Netw. **13**(4), 357–364 (2010)
16. Malik, S., Khan, M.: Impact of Facebook addiction on narcissistic behavior and self-esteem among students. J. Pak. Med. Assoc. **65**(3), 260–263 (2015)
17. Skues, J.L., Williams, B., Wise, L.: The effects of personality traits, self-esteem, loneliness, and narcissism on Facebook use among university students. Comput. Hum. Behav. **28**(6), 2414–2419 (2012)
18. Shaw, E., Ruby, K., Post, J.: The insider threat to information systems: the psychology of the dangerous insider. Secur. Awareness Bull. **2**(98), 1–10 (1998)
19. Schultz, E.E.: A framework for understanding and predicting insider attacks. Comput. Secur. **21**(6), 526–531 (2002)
20. US-CERT "Combating the Insider Threat", National Cybersecurity and Communications Integration Center, May 2014
21. Cummings, A., et al.: Insider threat study: Illicit cyber activity involving fraud in the US financial services sector. No. CMU/SEI-2012-SR-004. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst (2012)
22. Kowalski, E., Cappelli, D., Moore, A.: Insider threat study: illicit cyber activity in the information technology and telecommunications sector. Carnegie Mellon University, Software Engineering Institute (2008)
23. Golbeck, J., et al.: Predicting personality from twitter. In: 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom). IEEE (2011)
24. Back, M.D., et al.: Facebook profiles reflect actual personality, not self-idealization. Psychol. Sci. **21**(3), 372–374 (2010)
25. Alahmadi, B.A., Legg, P.A., Nurse, J.R.C.: Using internet activity profiling for insider-threat detection (2015)
26. Ackerman, D., Mehrpouyan, H.: Modeling human behavior to anticipate insider attacks via system dynamics. In: Proceedings of the Symposium on Theory of Modeling and Simulation. Society for Computer Simulation International (2016)
27. Greitzer, F.L., Frincke, D.A., Zabriskie, M.: Social/ethical issues in predictive insider threat monitoring. Inf. Assur. Secur. Ethics Complex Syst.: Interdisc. Perspect 132–161 (2010)
28. Sarkar, K.R.: Assessing insider threats to information security using technical, behavioural and organisational measures. Inf. Secur. Tech. Rep. **15**(3), 112–133 (2010)
29. Chen, Y., et al.: Leveraging social networks to detect anomalous insider actions in collaborative environments. In: 2011 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE (2011)
30. SANS Technology Institute, The 6 Categories of Critical Log Information. http://www.sans.edu/cyber-research/security-laboratory/article/sixtoplogcategories. Accessed 06 Jan 2017
31. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D.: An insider threat prediction model. In: Katsikas, S., Lopez, J., Soriano, M. (eds.) TrustBus 2010. LNCS, vol. 6264, pp. 26–37. Springer, Heidelberg (2010). doi:10.1007/978-3-642-15152-1_3

32. Kandias, M., et al.: Proactive insider threat detection through social media: the YouTube case. In: Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society. ACM (2013)
33. Kowalski, E., et al.: Insider threat study: illicit cyber activity in the government sector. In: US Department of Homeland Security, US Secret Service, CERT, and the Software Engineering Institute (Carnegie Mellon University), Technical report (2008)
34. O'Connor, B.P., Dyce, J.A.: A test of models of personality disorder configuration. J. Abnorm. Psychol. **107**(1), 3 (1998)
35. Caci, B., et al.: Personality variables as predictors of Facebook usage. Psychol. Rep. **114**(2), 528–539 (2014)
36. Ortigosa, A., Carro, R.M., Quiroga, J.I.: Predicting user personality by mining social interactions in Facebook. J. Comput. Syst. Sci. **80**(1), 57–71 (2014)
37. Styles, M., Tryfonas, T.: Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users. Inf. Manag. Comput. Secur. **17**(1), 44–52 (2009)