Proceeding of the 38th International Conference of the System Dynamics Society
Bergen, Norway, USA -- July 19-23, 2020

Insider Threat Dynamics; the dangerous triangle of pressure, rationalization and opportunity

Sander Zeijlemaker, PhD student Radboud University, IMR Faculty Nijmegen
Postbus 9108, 6500 HK Nijmegen, +31 6 29 46 84 89, s.zeijlemaker@fm.ru.nl

Key-words: insider threat dynamics, rationalization, pressure, opportunity

Extended Summary

It is known that cybersecurity costs and investments in security capabilities are going to increase over time. This makes an insider a very interesting target for threat actors because the insider has passed the boundary controls of the organisation. This also makes insider threat a concern for the defender.

In the field of insider threat-related research, the human psychology and human behaviour that evokes fraudulent behaviour has become of increasing scientific interest.

In the field of system dynamics, I observe the same development in research interests. The system dynamics models explaining insider threats are also more focussed on the human psychology and human behaviour that evokes fraudulent behaviour. Yet, this field follows the development of insider threat. Figure 1 shows a timeline of this development as well as my research contribution.

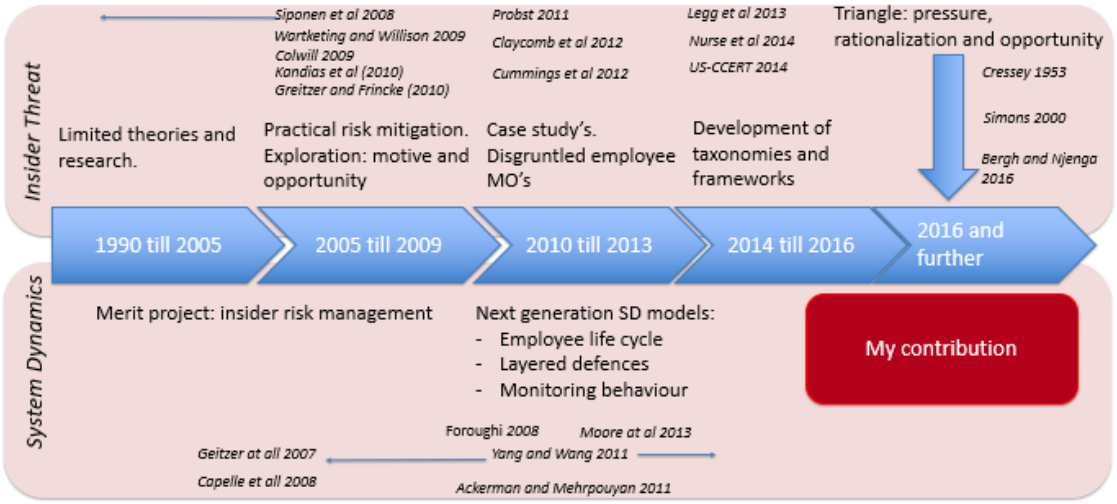

Figure 1. *Theory development overview and positioning of research contribution on Insider Threat*

My research in this paper explains the structure underlying the feared and preferred behaviour related to the number of insider threat cases over time and takes into account the factors of pressure, rationalization and opportunity. The presence of this triad may evoke fraudulent behaviour by insiders.

Figure 2 shows an aggregated insider threat model. This model will be explained below. The core of my model consists of non-fraudulent employees, potential fraudulent employees, and active fraudulent employees. In the first stage, employees are hired and not willing to commit fraud. These employees are called non-fraudulent employees. Once these employees perceive a certain level of pressure (fed by personal pressure, organisational pressure and work related pressure) rationalisation (influences by ethical behaviour and ethical training) about their behaviour, they will become employees who are willing to commit fraud. I call them potential fraudulent employees. When there is an opportunity to commit fraud, a fraction of them will actually commit fraud. These employees are called active fraudulent employees. In Figure 2 only the potential and active fraudulent employees are represented by threat actor. The other types of employees are not visualized.

This process of willingness to commit fraud will be influenced by different dynamics: namely, staff availability and work-related pressure (green), organizational change and pressure (purple), ethical behaviour and ethical training (orange), defences in place (blue), and attacker's behaviour (red). Figure 2 shows the contextual business layer of the insider threat architecture which is comparable with an sub sector diagram within the system dynamics field.

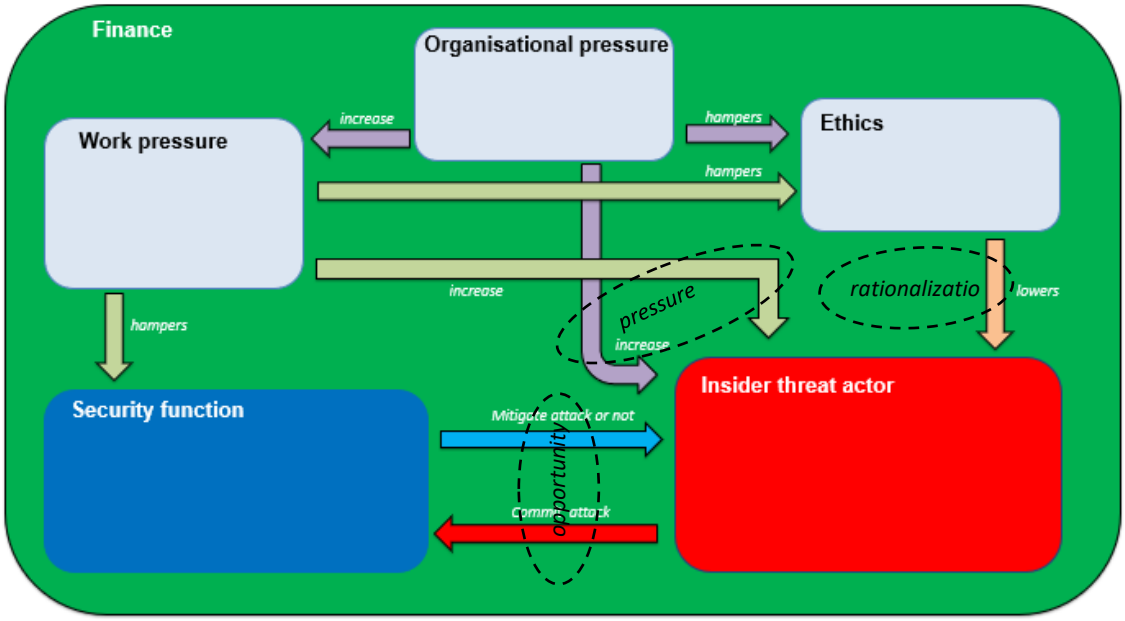

Figure 2. *Contextual business layer of the insider threat architecture where pressure, opportunity and rationalization are plotted..*

Although many controls are known, my research suggests more focus on ethics will contribute to the reduction of this threat. These controls include, amongst others, belief controls, tone at the top, ethical training, and speaking up. Limited studies consider pre-employment screening as well as appraisal and evaluation of employees as these controls may contribute to insider threat reduction as well.

More and more, organisations are working closely with other organisations, storing data in cloud solutions, and outsourcing activities. All these parties will have access to defenders' assets. As a result, the term insider will have a broader scope — one that's similar to the external insider. Franqueira, Van Cleeff, Van Eck, and Wieringa (2010) explain the phenomenon of the external insider. External insiders are parties who have earned the trust of the organisation, and may enter the networks, systems, data, and buildings of the organisation because of an agreement. An example of an external insider is a cloud provider or service provider (outsourcing) with higher trust levels and access to (parts) of the internal organisation. Also, certain malicious activities may happen without criminal intent (Van den Bergh and Njenga 2016). Both are relevant for future research in the field of insider threat.

Literature

Ackerman, D., & Mehrpouyan, H., 2016. Modelling Human Behaviour to Anticipate Insider Attacks via System dynamics, SpringSim-TMS/DEVS 2016 April 3-6, CA, USA, 2016, Society for Modeling & Simulation International (SCS).

Andersen, D., Cappelli, D.M., Gonzalez, J.J., Mojtahedzadeh, M., Moore, A., Rich, E., Sarriegui, J.M., Shimeall, T., Stanton, J., Weaver, E., & Zagonel, A., 2004. Preliminary System dynamics Maps of the Insider Cyber-threat Problem, System dynamics Conference, 2004.

Cappelli, D.M., Moore, A.P., Trzeciak, R.F., & Shimeall, T.J., 2009. *Common Sense Guide to Prevention and Detection of Insider Threat, 3rd Edition*—Version 3.1. Software Engineering Institute, Carnegie Mellon University and CyLab, 2009. http://www.cert.org/archive/pdf/CSG-V3.pdf

Cappelli, D.M., Desai, A.G., Moore, A.P., Shimeall, T.J., Weaver, E.A., & Wilke, B.J., 2008. *Management and Education of the Risk of Insider Threat (MERIT): System dynamics Modelling of Computer System Sabotage* May 2008, Carnegie Mellon University, Software Engineering Institute (SEI), Pittsburgh, PA,15213.

Cappelli, D.M., Desai, A.G., Moore, A.P., Shimeall, T.J., Weaver, E.A., & Wilke, B.J., 2007. *Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems, or Networks* —March 2007, TECHNICAL NOTE CMU/SEI-2006-TN-041, Software Engineering Institute, Carnegie Mellon University and CyLab.

Claycomb, W.R., Huth, C.L., Flynn, L., McIntire, D.M., and Lewellen, T.B., 2012. Chronological Examination of Insider Threat Sabotage: Preliminary Observations, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, volume: 3, number: 4, pp. 4-20.

Colwill, C., 2009. Human factors in information security: The insider threat- Who can you trust these days?, *Information Security Technical Report*, 14 (2009), 186 – 196.

Cressey, D.R., 1953. *Other People's Money*. Montclair, NJ: Patterson Smith, pp.1-300.

Cummings, A., Lewellen, T., McIntire, D., Moore, A.P., & Trzeciak, R., 2012. *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*, July, 2012, SPECIAL REPORT CMU/SEI-2012-SR-004.

Foroughi, F., 2008. The Application of System dynamics for Managing Information Security Insider-Threats of IT Organization, Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

Franqueria, V.N.I., Van Cleef, A., van Eck, P., & Wieringa R., 2010. External Insider Threat: A Real Security Challenge in Enterprise Value Webs, 2010 International Conference on Availability, Reliability, and Security.

Greitzer, F.L. & Frincke D.A., 2010. Combining Traditional Cybersecurity Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation, Part of the *Advances in Information Security* book series (ADIS, volume 49), 28 July 2010.

Greitzer, F., Moore, A., Cappelli, D., Andrews, D., & Carroll, L., 2007. Combating the insider Cyber threat, Published by the IEEE Computer society n 1540 7993/07/$25.00 ©2007, IEEE Security & Privacy.

Hunker, J. & Probst, J.W., 2011. Insiders and Insider Threats An Overview of Definitions and Mitigation Techniques, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 2011.

Legg, P., Moffat, N., Nurse, J.R.C., Happa, J., Agrafiotis, I., Goldsmith, M.,& Creese, S., 2013. Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, volume: 4, number: 4, pp. 20-37.

NCCIC/US-CERT, 2014. Combating the Insider Threat. NCCIC/US-CERT, USA.

Nurse, J.R.C., Buckley, O., Legg, P.A., Goldsmith, M., Creeese, S., Wright, G.R.T., & Whitty, M., 2014. Understanding Insider Threat: A Framework for Characterising Attacks, 2014 IEEE Security and Privacy Workshops.

Simons, R., 2000. *Performance Measurement & Control Systems for Implementing Strategy: Text & Cases*. Prentice Hall, Upper Saddle River, New Jersey 07458, 2000.

Warkentin, M. & Willison, R., 2009. Behavioural and policy issues in information systems security: the insider threat, *European Journal of Information Systems*, 18:2, 101-105, DOI: 10.1057/ejis.2009.12.

Van den Bergh, M. & Nienga, K., 2016. Information Security Policy Violation: The Triad of Internal Threat Agent Behaviour, Proceedings of the 1st International Conference on the Internet, cyber security, and information systems (ICICIS), Gaborone, 18-20 May 2016.

Yang, S.C., &Wang, Y.L., 2011. System dynamics Based Insider Threats Modeling, *International Journal of Network Security & Its Applications (IJNSA)*, **Vol.3**, No.3, May 2011, DOI : 10.5121/ijnsa.2011.3301.