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.

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


