CATCHING AN INSIDER SPY

The insider threat is a risk that comes from the people within the organisation, such as (ex-) employees, contractors, business partners and third parties (1). Some experts argue that employees are the biggest threat to companies, because they have legitimate credentials and access to data and systems which can cause much damage when abused (2). There are many definitions of the insider threat. The CERT Division of the United States Software Engineering Institute defines the insider threat as: "a current or former employee, contractor, or business partner who has or had authorized access to an organisation's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organisation's information or information systems" (1). The perpetrator is called a malicious insider.

One of the key aspects of a malicious insider, according to Eric Cole, an industry recognized security expert, is that they "have access and in most cases will exploit the weakest link that gives them the greatest chance of access, while minimizing the chances that they get caught" (2).

A good example of a malicious insider from the perspective of the US Government is Edward Snowden, who worked as a contractor with access to classified information. He was stationed at the NSA (3). Snowden downloaded thousands of classified NSA documents and leaked them to journalists (4) and allegedly to the Russian Government (5). The NSA is considered one of the most technologically sophisticated organisations in the world and failed to detect this incident (4).
A malicious insider can cause tremendous impact on an organisation, because malicious insiders may commit fraud, sabotage data or steal information like intellectual property (6). Stolen information can be sold to the highest bidder or leaked to competitors, which might hinder the competitive advantage of the organisation. Other negative effects include possible monetary loss of the organisation, financial instability, loss of customers and loss of customer confidence (2). Apart from the impact on the organisation, stolen information may indirectly pose a threat to its clients as well.

Acts of sabotaging data or stealing information are often part of (cyber)espionage (7). Espionage is the act of obtaining information considered secret or confidential using "human sources (agents) or technical means" (8). There are two different types of espionage: industrial espionage, which is conducted for commercial purposes, and international espionage, which is conducted by Government entities for the interest of the nation (9).

According to the Dutch General Intelligence and Security Service (AIVD), espionage is a serious threat for organisations in The Netherlands (7). They state on their website that Dutch organisations are structurally under espionage attacks and incidents have already occurred in a variety of sectors like the defence sector, the high-tech sector, the chemical and energy sector, the health sector and the water management sector (7).

To minimize (cyber)espionage risks, organisations are advised to implement mitigative controls (depending on their maturity level). These controls have in most cases a passive and restrictive nature, which means that they prevent espionage from happening to a certain extent. Mitigative controls include central log collection, network segmentation, network filtering,
access control and strict security policies.

The downside of this 'passive' approach is that the organisation only reacts after an incident is reported or a possible leak is discovered. There is a considerable chance that information can be stolen without the organisation taking notice.
A more active approach in identifying insider spies is needed. Therefore, the goal of this research was to develop a prototype of a technical system that can detect insider spies. By detecting insider spies in an early stage, the impact on the organisation can be minimalized. To achieve this goal, the following main research question has been formulated: "Which technical indicators of compromise can be defined and used to detect common behavioural traits and patterns of insider spies within organisations?"

To answer the research question multidisciplinary research was conducted. Insider spies have specific behavioural traits and patterns associated with their motivations and enablers (social science), which can (partly) be detected

Vincent de Vries is werkzaam bij Fox-IT als CISO en als manager van het Security, Quality en Compliance team. Hij heeft dit artikel geschreven op basis van zijn thesis voor de executive masteropleiding Cyber Security waar hij de technische track heeft gevolgd. In deze master gaat aandacht uit naar zowel technologische als juridische, bestuurskundige, economische en psychologische aspecten van digitale veiligheid. Vincent is te bereiken via devries@fox-it.com of via LinkedIn (linkedin.com/in/vincentdev)

by monitoring the technical systems they abuse (computer science).

Literature review and unstructured interviews with domain experts were carried out to establish the body of knowledge regarding insider spies. This research revealed multiple indicators of compromise, which might be used in identifying insider spy activity. Subsequently, exploratory data analysis was conducted based on the CRISP-DM process (10) on log data as a case study. This log data was provided by an organisation interested in benefitting from the results of the research and was anonymised before usage.

The goal of the exploratory data analysis was to determine the main characteristics of the collected log data, to prepare this log data for automatic analysis and to determine the value of the available log data in relation to the earlier defined indicators of compromise.
The data analysis provided multiple additional indicators and a good understanding of the relevance and value of the collected log data.
A prototype system was developed to automatically detect the defined indicators in the log data. This prototype was developed in line with the design-science research guidelines defined by Hevner et al (11).
This article describes the motivations, enablers, the behavioural traits and the patterns associated with insider spies. Furthermore, the article describes some indicators of compromise which can be used by organisations to gain more control on this threat.

Common motivations and enablers of insider spies

The first step in this research was to establish and explore the body of knowledge regarding insider spies. This contributed to the overall understanding of the insider spy threat and gave insights on how to detect their actions.

During the research four leading theories have been identified describing the motivations and enablers of insider spies. These theories are: 1) the five core motivations, 2) the suggested motives for spying (MICE), 3) the RASCLS framework and 4) the enablers and motivations of spying insiders identified by the FBI. These theories have been compared and merged during the research. Based on the comparison, the five core motivations have been extended with one additional core motivation.

The five core motivations were developed by Dr. Julie E. Mehan. These core motivations encourage and enable employees to become malicious insiders (regardless of the nature of the insider activity) (6). The five core motivations are: greed, ideology, ego, revenge and opportunity.

One of the most powerful motivators for insider threats is greed (6). Dr. Jeevan D'Souza defines greed as "the selfish desire to possess wealth, substances, objects, people, power, status, appreciation or attention far beyond what is required for basic human comfort" (12). According to the insider data collection study conducted by the British Centre for the Protection of National Infrastructure (CPNI), financial gain was the "single most common primary motivation" for malicious insiders (13) and was identified in 47 percent of the cases as the main motivator.

The research conducted by the CPNI, which is part of the United Kingdom's MI5 security service, included 120 UK-based insider cases from both the public and private sector (13), where there was significant damage to the organisation (13). The data analysis and collection took place between 2007 and 2012. The information on the incidents was collected by "reviewing case files, paperwork, and through formal interviews with key personnel who had knowledge of the individual" (13). A structured interview protocol was used to "ensure, where possible, the same type of information was captured for each case" (13).

The second core motivation is ideology which can be defined as a "set of beliefs about how the world or a set of behaviours should be" (6). Edward Snowden and Chelsea Manning are both examples where ideology seems to play an important role. Snowden released information because he feared a surveillance state (14), "to encourage other whistleblowers" (14) and because "he loves the concept of privacy" (15). Chelsea Manning released information "out of love for her country" and "a sense of duty to others" (16). According to the CPNI insider data collection study, ideology was the primary motivation in 20 percent of the studied insider cases (13).

The desire for recognition or retribution is at least greed's equal (6). According to the dictionary, ego is the "I or self of any person; a person as thinking, feeling, and willing, and distinguishing itself from the selves of others and from objects of its thought" (17). Malicious insiders felt disgruntled in some cases because they never received a response they believed they deserved (18). They "rationalize that their activities are justified" (6) and carry out their malicious act. According to the CPNI insider data collection study, in 14 percent of the cases, the desire for recognition was the motivator (13). David L. Charney claims in his paper titled 'True Psychology of the Insider

Insider spies tend to show certain behavioural traits and patterns before, during and after their malicious acts.

Spy' that injuries to human pride and ego are at the root of most cases of insider spying (19).

The fourth core motivator, revenge, is relatively uncommon for malicious insiders. It was the main motivator in only 6 percent of the cases studied by the CPNI (13). Malicious insider activities motivated by revenge often involve "acts of sabotage and unauthorized theft of intellectual property or government information" (6). An example of revenge can be found in the "Maroochy water breach". Vitek Boden worked for a company called Hunter Watertech that was responsible for the installation of the SCADA radio-controlled sewage equipment for the Maroochy Shire Council (20). In 1999 Vitek Boden left after disagreements with the company and tried to get a job at the local Council but was refused. Consequently he decided to take revenge on his previous employer and the Council by launching attacks on the radio-controlled SCADA sewage equipment (20). His attack caused "800,000 liters of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel" (20).

Opportunity, the fifth core motivator, is "a favourable juncture of circumstances" (21) and can be a motivation on itself, but mostly it only enables malicious insiders to commit their crimes. This is one of the enablers that can be controlled to a certain extent by the organisation itself. Organisations should have strict security controls, processes and procedures to inhibit and deter an employee's opportunity to commit a malicious insider action (22).

The comparison of the above-mentioned theories highlighted the absence of a sixth powerful motivation in the original five core motivations indicated by Dr. Mehan, the possibility of being influenced by a third party. Coercion is part of the suggested motives for spying (MICE) and influence can be exerted using the recruitment principles from the RASCLS framework.

Besides the motivations of an employee to become an insider spy, the organisation itself plays a part in enabling the would be spy. The organisation is in most cases the factor that motivates or provides opportunities to malicious insiders even though organisations might be justified and right in doing so (e.g. by treating the employee in a certain way). Malicious insiders can be motivated, amongst others, by poor management practices including a lack of management oversight, failure to address individual issues and failure to manage and resolve workplace issues (13). Due to the lack of management oversight, insider activities can be conducted either unnoticed or they are not addressed when noticed. Failure to address individual issues and failure to resolve workplace issues appear to contribute to the level of employee disaffection (13). Employee disaffection can escalate into employees taking revenge on the company.

Behavioural traits and patterns associated with insider spies

Insider spies tend to show certain behavioural traits and patterns before, during and after their malicious acts.

Behavioural traits

The CPNI, the FBI and the US-CERT focused on the workplace behaviour of an insider spy. They defined several suspicious workplace behaviours that might indicate that an employee is a malicious insider.

When an employee is engaged in unusual and unnecessary copying activities, this might be an indication of an insider spy. Unusual copying activities include copying sensitive files from servers, removing the classification from classified documents and copying printed documents at departments other than one's own (in the case a copier is available at the department of the employee) (13)(23)(24). It is also possible for an insider spy to, for example, photograph sensitive documents with a smartphone.

Another indicator can be found in unusual IT activity. This behaviour includes, amongst others, key-word based searches on subjects that are not related to one's work, in sensitive databases or on network shares (13)(23), increased computer usage shortly before foreign travel, using remote access functionality while on vacation, at odd times or when on sick leave (13)(23) and disregarding IT-policies by installing personal software or plugging private hardware in their computers (23).
Unauthorised handling of sensitive information might be an indicator. This includes storing and carrying sensitive

information without need or authorisation (13)(23). When an employee violates or ignores security policies, this might be an indicator as well (13).

Besides these behaviours, malicious insiders might show an unusual interest in matters outside the scope of their duties, particularly in foreign entities or business competitors in the case of espionage (24). They might have unexplained wealth (they buy things they cannot reasonably afford with their salary) (23) and they might take short trips to foreign countries for a limited amount of time for unclear reasons. They can show "unusual interest in personal lives of co-workers" (23) and they might be overly enthusiastic to work overtime, late at night, odd times or in the weekend (24). In some cases, malicious insiders have concerns that they are being investigated. They may leave traps to detect searches (23).

Insider spy patterns

The researched theories all focus on a specific part of the insider spy attack. The focus is either on the psychology of an insider or on the attack pattern the insider follows. During the research, it became evident that there is no model that combines both the psychology perspective and the attack pattern perspective of an insider spy attack. There is a clear gap between both views and it appeared to the researcher that only the FBI and the Institute of Electrical and Electronics Engineers (IEEE) tried to map the whole attack chain. However, they lack the psychology insights of the insider threat due to their focus on the attack pattern. To fully understand the insider spies and their attack patterns there is a need for a model that combines both views and that integrates those into a kill chain. This model should illustrate the phases and stages an insider spy attack passes, so organisations can take measures to minimalize the insider spy risk.
Based on the established body of knowledge through expert interviews and the extensive literature review, an insider spy kill chain was developed that illustrates the structure of an insider spy attack. This kill chain contains five phases including 14 stages and is illustrated in Figure 1. The phases in the model are: the Life Experiences phase, the Shift of Allegiance phase, the Attack Preparation phase, the Active Attack phase and the Post-Attack phase.

During the Life Experiences phase, the insider might develop predispositions which establish the basis for future decisions. This basis can enable or motivate an insider spy to commit a malicious act when experiencing multiple stressful life events in a short time period (25). Subsequently, during the Shift of Allegiance phase, the insider spy experiences multiple stressors, shows concerning behaviour and reaches a tipping point on which the insider spy will start with his/her malicious actions due to the earlier

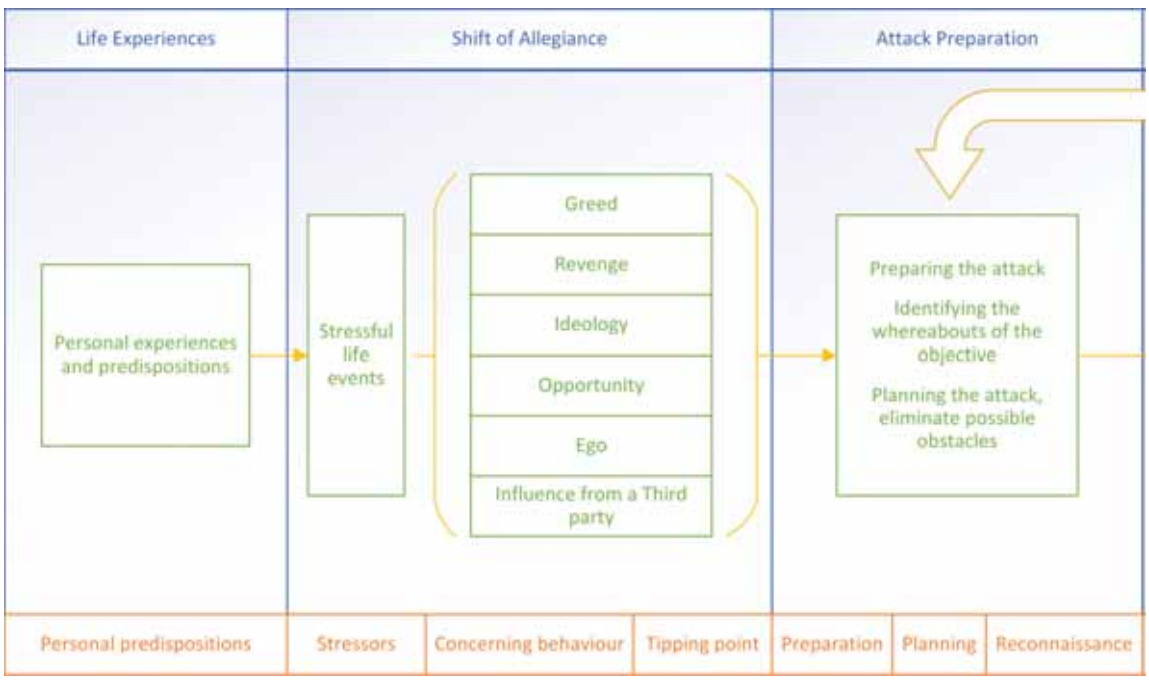


Figure 1 – The insider spy kill chain

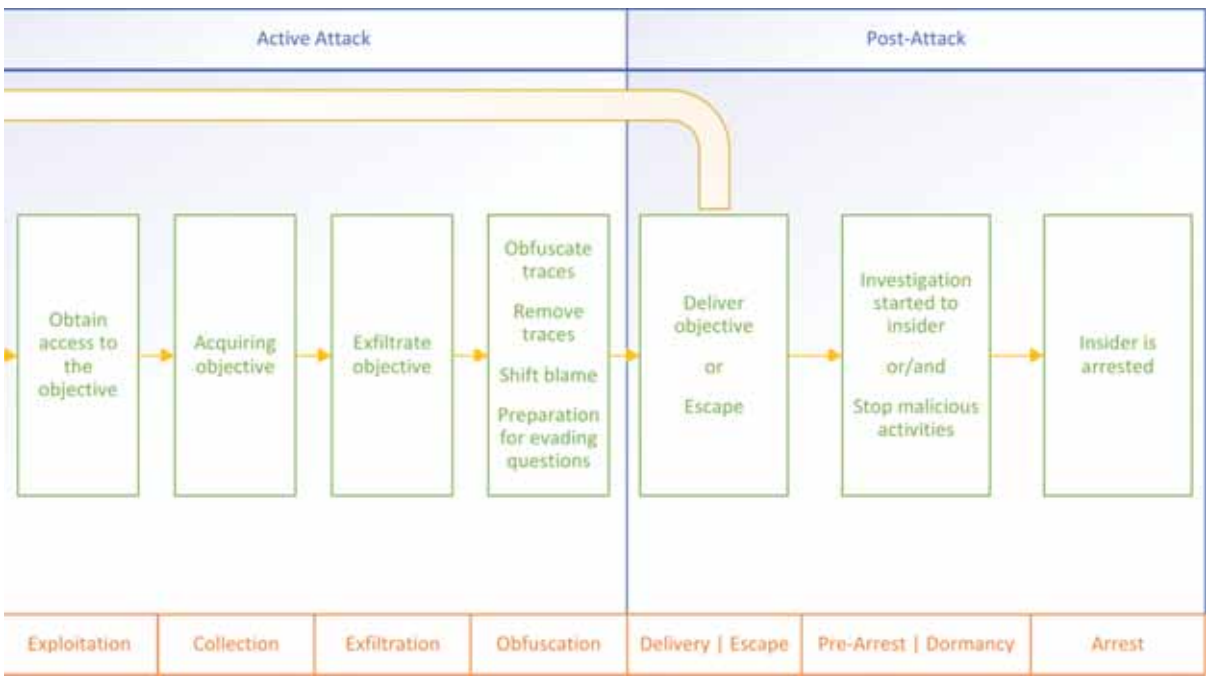
defined six core motivations and enablers for spying (greed, revenge, ideology, opportunity, ego and the influence from a third party).

During the Attack Preparation phase, the insider spy prepares the attack by deciding on a plan and will carry out reconnaissance if deemed necessary. This phase is followed by the Active Attack phase, during which the insider passes through four stages: exploitation, collection, exfiltration and obfuscation. In this phase the insider spy obtains access to the objective, acquires the objective, exfiltrates it and starts obfuscating the traces.

Finally, there is the Post-Attack phase, where the insider spy delivers the objective and/or escapes. After delivery the insider might be asked or feels obligated, in the case of an insider spy motivated by ideology, to collect/deliver more of the objective. That is why the kill chain has a possible loop back to the Attack Preparation phase. When an insider escapes or when colleagues notice suspicious behaviour, the organisation and authorities might start an investigation towards the insider spy. This is where the pre-arrest and dormancy stages described by Dr. D. Charney start (19). The insider might stop its previous activities in these stages or discover surveillance. Only one stage remains which is the arrest stage. During this stage the insider spy clearly did not escape and is successfully incarcerated and brought to justice.

It should be noted that the stages in the insider spy kill chain are not set in stone and some attacks might not encompass every stage. A good example is represented by the obfuscation stage because not all insiders will obfuscate their traces. The kill chain can end at any stage because the insider activity might be noticed and stopped upon detection. For example, during the data collection, technical indicators of compromise could notify the security team of suspicious behaviour which can be the start of an investigation. This means that at every stage, except the Personal Predispositions and the Arrest stages, an investigation can be started.

The first phase (Life Experiences) and the first and second stages of the second phase (Shift of Allegiance) are based on the research of Eric Shaw and Laura Sellers (25). The tipping point stage is based on the results of the literature review and the Attack Preparation phase is based on both the insider threat kill chains of the FBI (26) and the IEEE (27). This is also the case for the stages in the Active Attack phase and the first stage of the Post-Attack phase. The last two stages are based on the insider spy psychology studies of Dr. D. Charney (19).



Common indicators of compromise

This section gives a brief overview of a number of indicators of compromise associated with insider spies. It should be noted that these events or behaviours by themselves do not imply that an employee is an insider spy, although a combination of multiple indicators could be the starting point for an investigation.
The indicators of compromise come in many forms. Below is an overview of the indicators based on how and where they can be detected. Three categories were defined: indicators through social interaction and observations, indicators that can be observed depending on the context and lastly indicators through socio-technical and technical activities.

Social interaction and observations

The following indicators, amongst others, can be detected by employees through social interaction and observations:

- Unusual or unexplainable stress peaks
- Unexplained wealth
- Short trips to foreign countries for a limited amount of time
- Unusual interest in personal lives of co-workers
- Appearing intoxicated at work
- Pattern of significant change from past behaviour, especially relating to increased nervousness or anxiety (28)
- Deterioration of personal hygiene (28)
- Increased friction in relationships with co-workers (28)
- Enthusiastic to work overtime, late at night, odd times or in the weekend
- Pattern of lying and deception of co-workers or supervisors

Detection based on context

The list below contains indicators that can be detected by individuals or by a technical solution depending on where the insider spy activity takes place:

- Unusual and unnecessary copying activities
- Regularly printing on printers in other departments
- Removing data classification from documents or declassifying sensitive files without a good reason
- Attempting to circumvent or defeat security or auditing systems, without prior authorization from the system administrator, other than as part of a legitimate system testing or security research (28)
- Violating and/or disregarding security policies
- Attempts to enlist others in illegal or questionable activity

Socio-technical and technical activities

The list below contains indicators that can be used to detect suspicious socio-technical and technical behaviour:

- Using remote access functionality while on vacation, at odd times, odd locations (geoIP) or when on sick leave
- Access denied events related to specific zones in the organisation
- Discrepancy between usage of alarm code and physical access to the building
- Outliers in the number of bytes transferred to and from VPN clients
- Inconsistency between the time spent in the building and the declared working hours
- Access denied requests originating from a system assigned to a different user (applicable if all employees have a personal workstation)
- Outliers in privileged user account activities
- Outliers in the size of incoming and outgoing e-mail messages
- Forwarding of internal e-mails to an external e-mail address
- Outliers in file share activity regarding access attempts
- Discrepancy between usage of VPN connection and physical presence in the building

The general technical indicators of compromise from an external attacker must be taken into account as well because an insider spy might apply these techniques.
It should be mentioned that the results of the literature review are mostly based on research conducted in the United States and the United Kingdom. This means that the results of their research might not be fully applicable on malicious insiders in the Netherlands (due to cultural differences), although the results from the literature review and domain experts interviews apply well to six known Dutch insider cases. Further research should be conducted in this area.

Prototype system

The body of knowledge resulting from this research was implemented in a prototype system. The aim of the initial version of the prototype was to detect the technical indicators of compromise in the available datasets.
The results show that a prototype system can detect the defined indicators. The prototype was able to find some unusual events in the log data. However, to improve the prototype and the technical indicators of compromise, further research is needed.

Whether an insider spy will be detected by the organisation depends on his/her level of operational knowledge and security. In the case an insider receives instructions from an intelligence agency, or when an insider is trained by such an agency, operational mistakes are limited and it is likely that information is exfiltrated without detection.

(NB) Due to the size of this article, the results of the exploratory data analysis and the details regarding the prototype system had to be omitted. The researcher is preparing an additional article or blog post on this subject.

References

(1) D. Cappelli, A. Moore, R. Trzeciak, and T. J. Shimeall, 'Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1', Published by CERT, Software Engineering Institute, Carnegie Mellon University, www. cert. org, 2009.

(2) E. Cole and S. Ring, 'Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft', 1st ed. Syngress, 2006.

(3) 'Edward Snowden', Biography.com, www.biography.com/people/edward-snowden-21262897.

(4) 'Edward Snowden and the NSA: A Lesson About Insider Threats', Bloomberg.com, 03-Jul-2013, https://bloom.bg/2Knpfss.

(5) 'Was Edward Snowden a Spy? The Answer Remains Classified - Bloomberg', https://bloom.bg/2l4xQIK.

(6) J. Mehan, 'Insider Threat - A Guide to Understanding, Detecting, and Defending Against the Enemy from Within', 1st ed. IT Governance Ltd, 2016.

(7) M. van B. Z. en Koninkrijksrelaties, 'Cyberspionage - Cyberdreiging - AIVD', 10-Jun-2015, www.aivd.nl/onderwerpen/cyberdreiging/cyberspionage.

(8) 'Espionage | MI5 - The Security Service', https://www.mi5.gov.uk/espionage.

(9) I. Staff, 'Industrial Espionage', Investopedia, 29-Mar-2010, www.investopedia.com/terms/i/industrial-espionage.asp.

(10) R. Wirth and J. Hipp, 'CRISP-DM: Towards a standard process model for data mining', in Proceedings of the 4th international conference on the practical applications of knowledge discovery and data mining, 2000, pp. 29–39.

(11) A. R. Hevner, S. T. March, and S. Ram, 'Design science in information systems research', MIS Quarterly, vol. 28, no. 1, pp. 75–105, 2004.

(12) J. D'Souza, 'Greed: Crises, Causes, and Solutions', International Journal of Humanities and Social Science, vol. 5, no. 7, pp. 1–6, 2015.

(13) 'CPNI Insider data collection study - Report of main findings', Apr-2013, https://bit.ly/2Hz9fFY.

(14) K. Hill, 'Why NSA IT Guy Edward Snowden Leaked Top Secret Documents', Forbes, https://bit.ly/2I0YLyA.

(15) G. Greenwald, E. MacAskill, and L. Poitras, 'Edward Snowden: the whistleblower behind the NSA surveillance revelations', The Guardian, 11-Jun-2013.

(16) C. Manning, 'Chelsea Manning on the U.S. Military and Media Freedom', The New York Times, 14-Jun-2014.

(17) 'Ego | Define Ego at Dictionary.com', www.dictionary.com/browse/ego.

(18) 'Insider Threats 101: The Threat Within', TrendLabs Security Intelligence Blog, 09-Dec-2014, https://bit.ly/2I16Ymh.

(19) D. L. Charney, 'True Psychology of the Insider Spy', Intelligencer: Journal of U.S. Intelligence Studies, 2010.

(20) M. Abrams and J. Weiss, 'Malicious control system cyber security attack case study–Maroochy Water Services, Australia', McLean, VA: The MITRE Corporation, 2008.

(21) 'Definition of OPPORTUNITY', www.merriam-webster.com/dictionary/opportunity.

(22) Dawn Cappelli, Andrew Moore, and Randall Trzeciak, 'The CERT® Guide to Insider Threats - How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud'). Addison-Wesley Professional, 2012.

(23) 'The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy', Federal Bureau of Investigation, www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.

(24) U.S. Department of Homeland Security, Combating the Insider Threat', 02-May-2014.

(25) E. Shaw and L. Sellers, 'Application of the Critical-Path Method to Evaluate Insider Risks', Laos: Operation MILLPOND, 1961 Foundations of Anglo-American Intelligence Sharing The National Intelligence Council, 2009–2014 Evaluating Insider Risk–The Critical-Path Method, vol. 59, no. 2, p. 41, 2015.

(26) HackersOnBoard, 'BlackHat 2013 - Combating the Insider Threat at the FBI: Real-world Lessons Learned', www.youtube.com/watch?v=38M8ta13K0Q.

(27) J. R. C. Nurse et al., 'Understanding Insider Threat: A Framework for Characterising Attacks', in 2014 IEEE Security and Privacy Workshops, 2014, pp. 214–228.

(28) Antonio A. Rucci, 'Protecting Against and Investigating Insider Threats', presented at the Defcon 17, Las Vegas, 2017.