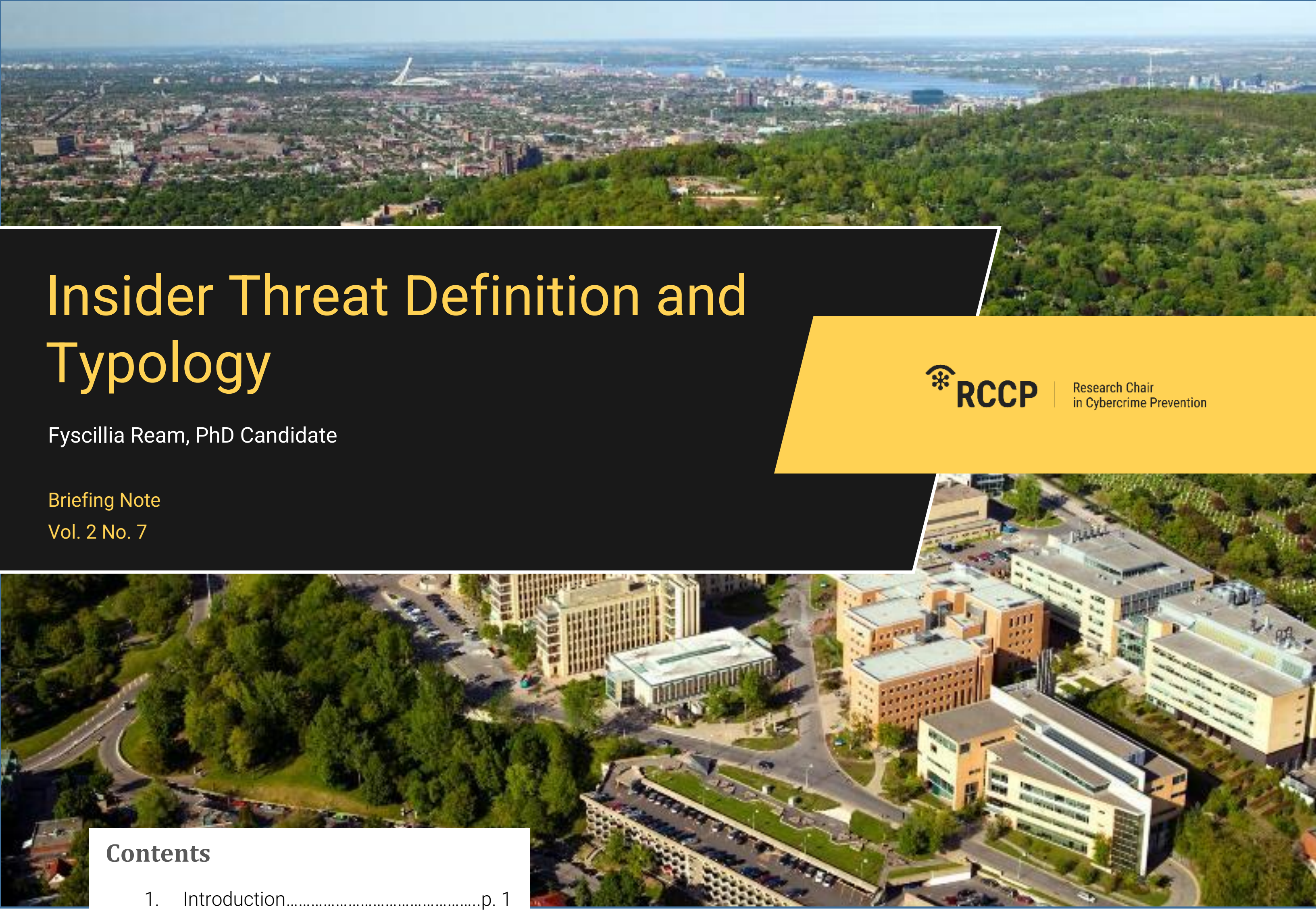


Insider Threat Definition and Typology

Fyscillia Ream, PhD Candidate

Briefing Note
Vol. 2 No. 7

RCCP | Research Chair in Cybercrime Prevention

Contents

The Research Chair in Cybercrime Prevention was created on the initiative of Université de Montréal, Desjardins and the National Bank of Canada. Headed by Benoît Dupont, a researcher at the International Centre for Comparative Criminology at Université de Montréal, its mission is to contribute to the advancement of research into cybercrime phenomena with a view to prevention.

Introduction

In cybersecurity, insider threat is cited as one of the most serious issues for organizations. While organizations face many more external attacks than insider threats, these have higher success rates. Indeed, insiders enjoy certain advantages that external cybercriminals do not. Insiders are familiar with how their target's computer systems work and know the security countermeasures their employers have put in place.[1, 2, 3]

A 2018 Verizon report stated that 20% of cybersecurity incidents reported by the organizations surveyed were the result of inappropriate use of technology by employees, and that 15% of data breaches were the result of an insider threat event.[3]

Insider threat is a difficult issue to manage for organizations, which lack knowledge about them. A 2017 survey shows that only 18% of Canadian businesses have established a definition of insider threat, up slightly from 2012, when 14% of businesses had defined insider threat.[4]

Organizations focus almost exclusively on external attacks, in part because security audit tools and modelling techniques are already available, helping to detect and manage vulnerabilities. Moreover, insider threat design is often based on erroneous models because it is difficult to measure. The lack of detection tools and techniques also contributes to the confusion around this phenomenon.[2]

It is therefore important for organizations to define insider threat so that they can implement appropriate responses to better manage this issue. This briefing note presents the aspects to be considered in defining insider threat and illustrates typologies from the scientific literature.

Defining insider threat

Despite interest in insider threat issues in recent years, definitions in the research are inconsistent.[5] The Computer Emergency Response Team/Coordination Center (CERT/CC) defines insider threat as "the potential for an individual who has or had authorized access to an organization's [physical and non-physical] assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization." However, while the CERT is a recognized reference for insider threat, this definition is not used in all studies. The following elements from other definitions should also be considered.

Insider: In English, the individual responsible for the threat is called an "insider." In French, the term *initié* best reflects this terminology. According to the *Larousse* French dictionary, an insider is "someone who operates in secret, is aware of certain practices and is educated in some art" [translation].[6] The *Merriam-Webster* defines an insider as "a person recognized or accepted as a member of a group, category or organization, such as (a) a person who is in a position of power or has access to confidential information; (b) a person who is in a position to have special knowledge of the affairs of or to influence the decisions of a company."[7] "Insider threat" therefore involves an individual who has specific knowledge or confidential information and whose actions pose a threat to the organization.

An insider can be[5, 8, 9, 10, 11, 12]:

- An employee (current, former or temporary), a student intern or another member of an organization who has access to the IT system;
- A trusted person who has access to critical information;
- A person who has privileged access;
- An associate, consultant, business partner, supplier, IT service engineer, guest, client or person having a formal or informal relationship with the organization;
- Any person authorized to carry out certain activities or any person properly identified and authenticated in the system;
- A former insider (employee, supplier, partner, etc.) who uses revoked access credentials or covertly creates credentials for use after their departure;
- An employee whose credentials have been compromised and are being used by an external person.

Threat: Unintentional errors are often perceived as inevitable, while malicious behaviour is perceived as dangerous and needing to be prevented.[9] However, distinguishing acceptable and unacceptable insider behaviour can be difficult and context dependent. Threat represents all acts committed or potentially committed that endanger the organization's operations. Most studies focus only on hazards in an organization's IT environment and ignore the physical aspect of threats, that is, acts that can be committed in the organization's physical environment. Threat also depends on organizations and how they operate. If an organization uses few sensitive physical documents, then the loss of these documents is unlikely to represent a significant risk. However, sending sensitive information by email by mistake or malicious intent may pose a more likely threat to the organization.

Trust: Several definitions of insider threat emphasize the notion of trust. Insider threat occurs when an organization trusts an employee to protect its information and assets, and that employee (insider) fails to do so, losing the trust placed in them. Organizations must therefore be able to determine whom they can or cannot trust. Organizations also need to create a climate of trust to mitigate the risks associated with insider threat. Insiders are more likely to maintain the trust placed in them by the organization if they feel they can trust the organization in return. This reciprocity is expressed by establishing and maintaining a culture of trust based on strong values, ethical behaviours and consistent and transparent leadership.

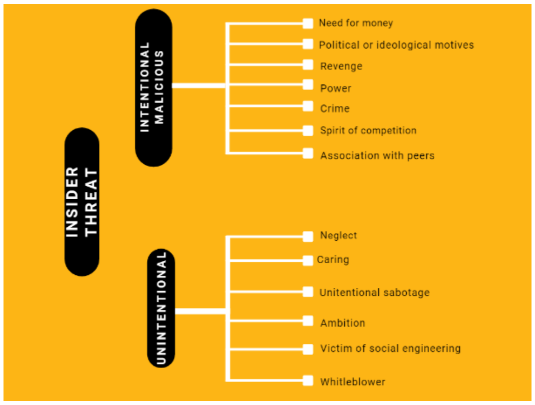
Parameters: The notion of parameters is also important because insider threat falls within the scope of an insider's actions. Parameters define the extent of an individual's scope of action within an organization. For example, in physical security, parameters represent the organization's physical locations, whereas in information security, an insider acts within parameters defined by the security architecture and policies.[13] The advent of mobile computing, cloud computing, outsourcing, the increasing use of contractors and even telework have blurred the boundaries of these parameters. Some definitions consider only the IT parameters in which an insider can act.[5] Few definitions consider physical parameters, which can bias insider threat management. For example, a maintenance officer may be an insider even if they do not have access to computer data, and remote employees may also be insiders, even if they are not physically present in their employer's offices.[2]

Security policy: In some definitions, insider threat occurs when there is a breach of security policies, that is, when a trusted individual violates one or more security policy rules. A security policy sets out rules about what is and isn't permitted. The definition of insider threat must therefore consider that an insider acts within a set of rules.[5]

Access: Some definitions emphasize that an insider must have access to data and, more specifically, privileged access to data. An insider therefore has login details giving them access to the organization's computer system and data. An individual who does not have access to data thus cannot pose a threat under these definitions.

Knowledge: Some studies emphasize that an insider must have specific knowledge, including IT knowledge of security controls and the organization's internal and IT operations. These definitions should be taken with a grain of salt, in that they focus on individuals who have technical knowledge without considering those who do not, but who nevertheless have privileged access.[14]

Insider threat typology



Unintentional insider threat

Definition

The CERT[15] defines unintentional insider threat as "a current or former employee, contractor or business partner who has or had authorized access to an organization's network, system or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity or availability of the organization's information or information systems." This definition includes all actions such as human error and any other incidents that may compromise the organization.[10] An action can cause damage even if it was well intentioned, such as when employees circumvent safety rules to improve productivity. For example, an insider could expose the organization to risks by making naive mistakes, visiting malware-infected websites, responding to phishing emails or using unsecured passwords.[16]

Actions

According to the CERT, unintended insider threat can be divided into 4 categories[15]:

- Inadvertent disclosure of sensitive information: An employee may post, email, mail or fax confidential information to the wrong recipients or mismanage it. In other cases, and for convenience, data may be transferred from a secure to an unsecured location, such as from the workplace to the home onto personal computers that are not properly secured.
- Hacking: When an employee falls victim to a social engineering attack that results in data theft or the installation of malware, ransomware and spyware.
- Non-compliant disposal of physical records, which may include loss or theft.
- Loss, non-compliant disposal or theft of portable devices (laptops, smartphones, external hard drives, etc.) containing confidential and sensitive data.

Two configurations increase the risk of unintended insider threat:[17]

- Mismanagement of data shared with trusted third parties: Partners (vendors, external consultants, etc.) without secure systems can put the organization at risk by acting as a gateway for external attacks.
- Forgetting to reconsider access: System administrators may forget to remove access from employees or other individuals who are no longer part of the organization.

Warnings

Employee motivations in cases of insider threat are important to consider, as managers' responses will differ depending on the case. A manager can sympathize with an employee who has broken rules to perform their duties more effectively but can also reprimand or even dismiss an employee who acts with malicious intent.[9] In cases of unintentional insider threat, the following motivations can be identified:

- Making an error under pressure from external factors, including a lack of time;
- Trying to perform tasks by accessing certain data to which you may not necessarily have access;
- Trying to ensure that the computer system can perform tasks for which it was not designed;
- Looking for vulnerabilities, weaknesses or errors in the system, intending to report them;
- Accessing data out of curiosity or boredom.

Typology

There are generally two categories of unintentional insider threat:[17]

Careless insiders/careerists: These insiders have legitimate access to a computer system and are trying to find ways to make their work easier. They are loyal to the organization but tend to follow only the policies and regulations that suit them. They violate security policies to improve their productivity.

Caring/altruistic insiders: These are often good employees who want what is best for the organization and, to achieve the organization's goals, do things that may pose a threat.

More specifically, these two general categories are divided into four profiles, according to what insiders do:

- Saboteurs: These insiders regularly undermine computer systems through their non-malicious actions. They use simple passwords or reuse the same password to authenticate themselves on multiple accounts. They may also write their passwords on Post-its on their screen or share them with colleagues.

- Go-getters: These insiders understand the importance of security but still take risks to get around security red tape and be more efficient and productive in advancing their careers. They may be take a cue from the organization's ethics if they emphasize success and results over security. For example, to save time go-getters will not encrypt data.

- Social engineering victims: These are employees who may be manipulated by external cybercriminals and who will then share sensitive information or provide access to the organization's computer systems. They may respond positively to phishing emails or share information because they think it will help the organization.

- Whistleblowers: These insiders will publicly disseminate some of the organization's data through anonymous social network technologies, such as WikiLeaks, whether for ethical reasons or not. Although they act against the interests of the organization and often illegally, they may be considered well intentioned when they are guided by the public interest and disclose illegal or immoral decisions or behaviour within their organizations.

Intentional/malicious insider threat

Definition

Intentional or malicious insider threat refers to situations where an employee, former employee, contractor or business partner who has or had privileged access intentionally uses it to undermine the confidentiality, integrity and availability of information, organizational systems and infrastructures.[10, 18] Typically, this insider will seek to exploit their privileged access for inappropriate gain (personal or financial) or revenge.[10]

Actions

According to the CERT,[18] malicious insider threat can be divided into 3 categories:

- Sabotage: This is any instance where an insider puts the organization at risk. An insider may, for example, search for security vulnerabilities to abet criminal acts.[19]

- Intellectual property theft: When an insider engages in espionage for a third party or steals data for personal use (for example, to start their own business) or for a third party (for example, as part of a job change).

- Fraud: This type of threat occurs when an insider modifies, falsifies or removes data from the organization to divert funds for their own benefit or that of third parties.

Motivations and typology

In cases of intentional/malicious insider threat, insiders have several possible motivations[19, 20, 21]:

- Need for money: Whether out of greed, to support an addiction (drugs, shopping, etc.) or an extravagant lifestyle (expensive clothing, multiple trips, etc.), to pay off debts, manage personal difficulties or respond to coercion or blackmail by someone inside or outside the organization, insiders needing money will seek financial gain by defrauding or stealing data for resale. These insiders are fully aware of the organization's operations and security policies and use their privileged access to access data by exceeding their permissions or stealing data.

- Political or ideological reasons: This motivation is found mainly in cases of sabotage and espionage on behalf of a foreign power or an extremist group.
- Desire for revenge: These insiders are unhappy with how the organization treated them after failing to get the promotion, increase or transfer they wanted.
- Power: These insiders feel entitled to commit mischief because of their role within the organization (high hierarchical position, etc.).
- Criminal activities: This motivation refers to employees who are career criminals. They change jobs to commit crimes. These individuals often begin their crimes shortly after they begin work. They are greedy, exploit others and use the stolen login details of co-workers to commit their crimes.
- Spirit of competition: Insiders want to prove to themselves or others that they are capable of committing mischief without being detected. These may be employees who commit wrongdoing solely to demonstrate intellectual and cognitive superiority. In these cases, insiders have advanced computer knowledge that allows them to access the system undetected.

Association with peers: This category includes groups of friends of similar ages working together on mischief. They sometimes operate hand in hand with external parties. They often commit a crime because they have seized an opportunity and encourage one another. They often demonstrate strong solidarity within the organization.

Study recommendations and limitations

The lack of a consistent definition of insider threat makes it difficult to implement threat detection measures.[5] By having a definition that considers all aspects relevant to the organization, decision-makers will be able to put in place appropriate risk detection and management measures. It is therefore essential for organizations to define insider threat in their policies, within their own specific parameters. The various definitions covered in this briefing note can give managers food for thought in identifying the issues specific to their organizations.

Studies on insider threat primarily provide insight into cases of observed insider threat or attempt to identify means (technology through the implementation of psychosocial or detection systems and algorithms) for predicting insider threat cases. However, trying to determine the profile of an insider who might present a threat begs the question of whether there is a typical insider profile. Early detection of insider threat is difficult and relying on psychosocial factors can generate a high number of false positives, pose privacy issues for employees[9] and create mistrust among these employees.

Moreover, the vast majority of these studies on insider threats come from computer science and suggest that insider threat is a technology-only problem. This implies, on the one hand, that insider threat is interpreted only in an IT context, and, on the other, that only computer technology can prevent and detect such cases. Obtaining accurate data on insider threat remains a challenge because, as we have seen, there is no consensus on its definition. It can also be difficult to distinguish unintentional and malicious actions.[5] Empirical data on insider threat is still limited, and where it does exist, it is often restricted to a particular organization and therefore only solves the problems specific to that organization.[11]

Another difficulty is the reluctance to share information. Due to privacy laws and a concern for corporate reputation, some organizations that have collected data on insider activity are reluctant to share it with other organizations to help them learn generalizable lessons.[9]

References

[1] Bishop, M. (2006). Position: insider is relative. NSPW '05: Proceedings of the 2005 workshop on New security paradigms, September 2005, 77–78.

[2] Chinchani, R., Iyer, A., Ngo, H. Q. and Upadhyaya, S. (2005). Towards a theory of insider threat assessment. Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05)

[3] Verizon Business. (2018). Data breach investigations report. Verizon Business.

[4] Newswire. (October 29, 2018). The Insider Threat: Majority of Canadian Organizations Still Unclear on What it Means. Newswire

[5] Bishop, M. and Gates, C. (2008). Defining the insider threat. CSIIRW '08: Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, May 2008, 1–3.

[6] Larousse. (n.d.). Inité, initiée.

[7] Merriam Webster. (n.d.). Insider.

[8] Brackney, R. and Anderson, R. (2004). Understanding the Insider Threat. Proceedings of a March 2004 workshop. Technical Report. RAND Corporation: Santa Monica, CA.

[9] Pfleeger, S.L., Predd, J.B., Hunker, J. and Bulford, C. (2010). Insiders Behaving Badly: Addressing Bad Actors and Their Actions. IEEE Transactions on Information Forensics and Security, 5(1), 169–179.

[10] Nurse, J.R.C., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R.T. and Whitty, M. (2014). Understanding Insider Threat: A Framework for Characterising Attacks. 2014 IEEE Security and Privacy Workshops, 215–228.

[12] Hamin, Z. (2000). Insider cyber-threats: Problems and perspectives. *International Review of Law, Computers & Technology*, 14(1), 105–113.

[14] C.W. Probst, J. Hunker, D. Gollmann and M. Bishop, 2010. Aspects of Insider Threats. In Insider Threats in Cyber Security. *Advances in Information Security*, 49, 1–15.

[15] CERT (2013). Unintentional Insider Threats: A Foundational Study. Pittsburg, PA: Carnegie Mellon University.

[16] Gundu, T. and Flowerday, S. V. (2012). The enemy within: A behavioural intention model and an information security awareness process. 2012 Information Security for South Africa, Johannesburg, Gauteng, 1–8.

[17] Wall, D.S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, 26(2), 107–124.

[18] Cappelli, D.M., Moore, A.P. and Trzeciak, R.F. (2012). The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Boston, MA: Addison-Wesley Professional.

[19] Whitty, M.T. (2018). Developing a conceptual model for insider threat. *Journal of Management and Organization*, 1–19.

[20] Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. and Ochoa, M. (2019). Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Comput. Surv.*, 52(2).

[21] Liu, L., De Vel, O., Han, Q., Zhang, J. and Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Communications Surveys & Tutorials, 20(2), 1397–1417.

[8] Brackney, R. and Anderson, R. (2004). Understanding the insider threat. Proceedings of a March 2004 workshop. Technical report. RAND Corporation: Santa Monica, CA.

[9] Pfleeger, S. L. , Predd, J. B., Hunker, J. and Bulford, C. (2010). Insiders behaving badly: Addressing bad actors and their actions. IEEE Transactions on Information Forensics and Security, 5(1), 169–179.

[10] Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T. and Whitty, M. (2014). Understanding Insider Threat: A Framework for Characterising Attacks. 2014 IEEE Security and Privacy Workshops, 215-228.

[12] Hamin, Z. (2000). Insider cyber-threats: Problems and perspectives. International Review of Law, Computers & Technology, 14(1), 105–113.

[14] C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop. 2010. Aspects of insider threats. In Insider Threats in Cyber Security. Advances in Information Security, 49, 1–15.

[15] CERT. (2013). Unintentional Insider Threats: A Foundational Study. Pittsburg, PA: Carnegie Mellon University.

[16] Gundu, T. and Flowerday, S. V. (2012). The enemy within: A behavioural intention model and an information security awareness process. 2012 Information Security for South Africa, Johannesburg, Gauteng, 1–8.

[17] Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. Security Journal, 26(2), 107–124.

[18] Cappelli, D.M., Moore, A. P. and Trzeciak, R. F. (2012). The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Boston, MA: Addison-Wesley Professional.

[19] Whitty, M. T. (2018). Developing a conceptual model for insider threat. Journal of Management & Organization, 1–19.

[20] Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. and Ochoa, M. (2019). Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. ACM Comput. Surv., 52(2).

[21] Liu, L., De Vel, O., Han, Q., Zhang, J. and Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. IEEE Communications Surveys & Tutorials, 20(2), 1397–1417.