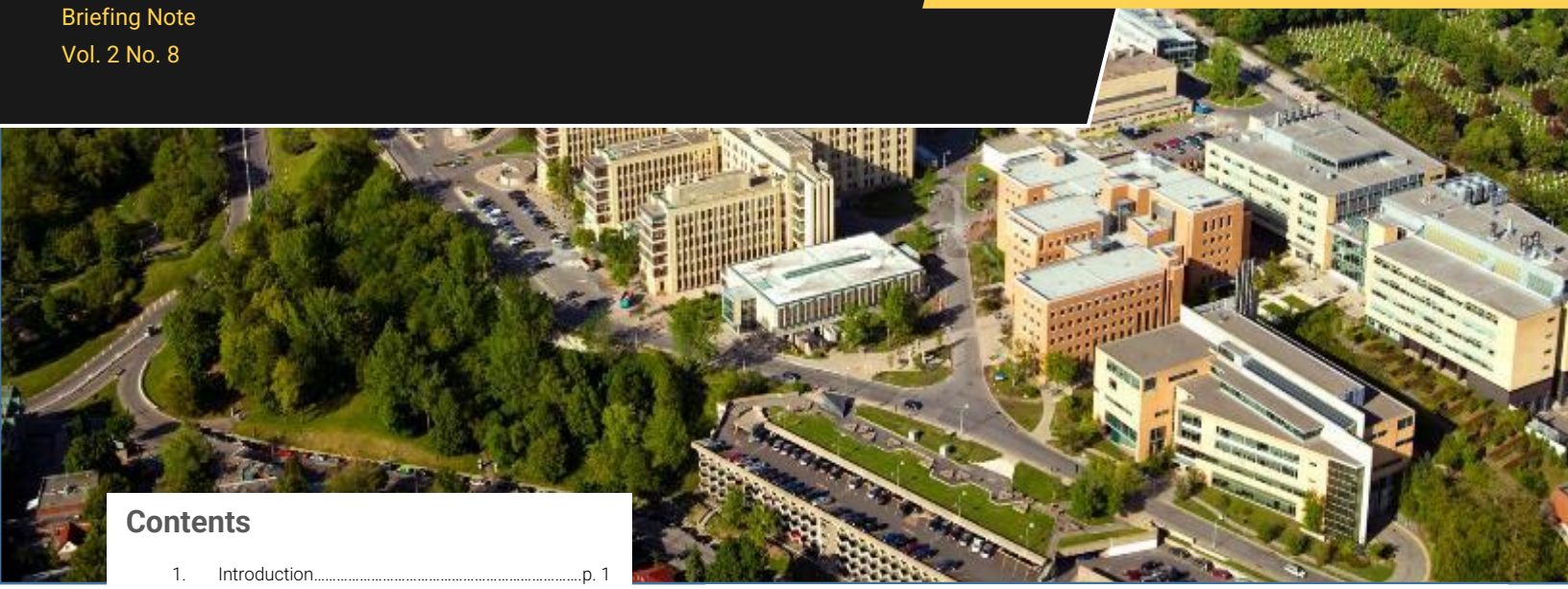
# Insider Threat Risk Factors

Adeline Veyrinas, MSc

Briefing Note
Vol. 2 No. 8

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

Insider threats are "**threats posed by individuals who intentionally or unintentionally destroy, exfiltrate or leak sensitive information, or expose their organization to outside attacks.**"[1] These individuals cause harm to their business through their behaviour. These increasingly frequent incidents represent **the second-biggest threat to cybersecurity**, after external hacking. They're also the costliest for organizations.[2, 3] In two years, the number of insider threat incidents increased by 47% and their cost to businesses increased by 31%.[4] This includes direct costs due to an incident such as financial, operating or reputational losses, as well as indirect costs such as for legal defence or systems repair.

Intentional insider threats can be expressed through a wide range of acts such as espionage, sabotage, misappropriation of funds, extortion or corruption.[5, 6] Unintentional threats can take the form of disclosure of login credentials following a social engineering attack or intrusion on portable equipment due to an unsecured network connection.[5]

These threats can have a significant impact on businesses, causing major financial losses or tarnishing their reputation.[7] Therefore, ideally, they should be managed upstream as part of a prevention strategy.

However, this presents a very real problem, namely that it's often difficult to identify the causes and behaviours that signal an insider threat.[1] Observable behaviours that may indicate whether or not an individual represents an insider threat are extremely varied, and their presence doesn't necessarily mean that there will be an insider attack. Furthermore, when an insider threat is unintentional, it may be difficult to identify the exact causes as the acts in question are merely errors that don't necessarily have specific reasons or motivations. However, the few studies on the subject have identified certain risk factors (insider threat causes). Knowing them and taking into account certain issues, it is possible to make practical recommendations that businesses can implement.

## Organizational risk factors

### Work environment

A number of risk factors related to a company's work environment have been identified as potential causes of insider threat. The most important of these are the following:

- Security policies/procedures: Lack of clarity, ineffective communication to employees and failure to adjust working conditions inhibit secure behaviours.[6, 8, 9, 10, 11, 12]

- Technological tools: Difficulty using these tools, poor adaptation to employee tasks and lack of security in their design all serve to increase risk.[9, 10, 12]

- Immediate environment: Noise, temperature, interpersonal conflict and office facility ergonomics can also influence insider threat.[10, 14, 15]

- Managerial practices: The number of tasks to be performed and/or intense pressure to perform them, poor communication between managers and employees, and a mismatch between job requirements and the knowledge and abilities of employees can also play a significant role.[6, 8, 9, 10, 14, 16, 17, 18]

All of these elements can lead to potential insider threat situations in two ways:

- Problems related to technological tools and security regulations can lead to risky behaviours or inappropriate decision-making, such as avoiding tools that are too difficult to use or not knowing what behaviours to adopt.[12, 13, 19]

- All of these risk factors can lead to disturbing emotions or feelings, such as overexertion, stress, anxiety or fatigue. This can in turn affect the performance of the employees involved and/or cause them to make mistakes, making them more likely to be victims of social engineering.[9, 10, 17, 18, 19, 20, 21, 22, 23] It can also bring about emotions/feelings of discontent or dissatisfaction and can affect employees' morale and attitude toward their employer. They could as a result deliberately engage in behaviours that are contrary to the well-being of the company.[3, 6]

### Organizational culture

Organizational culture embodies "a distinctive pattern of thought and behavior shared by members of the same organization and reflected in their language, values, attitudes, beliefs, and customs."[24] Two situations may pose an insider threat risk:

- Company culture: During times of significant change in the structure and/or management of the business, the transition may be quite abrupt. For example, new management with a different approach to security may reorganize or introduce new procedures without taking into account the existing organizational culture.

- Regional culture: In situations where the organization has branches in different regions, the company's rules, management, working conditions or guidelines may differ

from and conflict with the culture of local employees. In addition, language differences can sometimes lead to discrepancies between what's communicated and how it's perceived and interpreted, based on the culture of those involved.[25]

These organizational culture issues can lead to a number of insider threat situations:

- **Negative emotions**, such as fear, uncertainty or doubt, that can make individuals more likely to make mistakes and consequently fall victim to social engineering.[21, 25]

- **Tension between employees and their company** combined with feelings of neglect or lack of recognition, which can lead to increased susceptibility to errors and/or negative attitudes toward the organization.[11, 21, 26]

- In addition to possible tensions, employees may feel a **lack of identification** with the company that can lead to disengagement and indifference.[5] This can cause individuals to deliberately engage in behaviours that are contrary to the well-being of the business.[25]

## Individual risk factors

### Psychological factors

There are three broad categories of psychological factors that can negatively affect the employees of a business:

- **The Big Five model**, which defines an individual's personality according to five prevailing major traits. These include **openness** (openness to experiences), **conscientiousness** (order, discipline, organization), **extraversion** (energy, positive emotions), **agreeableness** (sociability, benevolence) and **neuroticism** (emotional instability, negative emotions). Some of the traits in this model have been clearly identified as potentially having a role in the development of insider threat, notably **agreeableness, neuroticism, openness and extraversion when these traits present positively** (the more the individual presents this trait, the more at risk they are), and **conscientiousness when it presents negatively** (the less the individual presents this trait, the more at risk they are).[5, 7, 27, 28, 29, 30, 31] However, the involvement of these traits in cases of insider threat remains to be verified, according to some, and differs depending on the individual and the type of threat in question. While agreeableness and conscientiousness have been shown to be a factor in cases of verified insider threat, neuroticism can, in contrast, contribute to the absence of insider threat when it involves computer-related anxiety leading to decreased use of networked technologies.[29] Moreover, these traits aren't immutable, and certain events in an individual's life may influence them one way or the other, which can in turn influence the risk of insider threat. For example, a history of falling for scams might negatively influence a person's agreeableness and, subsequently, their susceptibility to falling victim to social engineering.[32]

- **Affect**, which refers to the types of emotions that individuals can experience and the different moods that are associated with them. Thus, certain affect traits, particularly negative ones, have been identified as playing a certain role in the appearance of behaviours and/or circumstances of insider threat, such as misappropriation of company property, drug/alcohol use in the workplace and absenteeism.[28] The affects generally identified in these cases are hostility, sadness, fear, low self-esteem, shyness or inattention.[5, 7]

- **The dark triad** personality traits, namely **narcissism** (grandiosity, egotism), **Machiavellianism** (manipulation, amorality) **and psychopathy** (impulsivity, lack of empathy) that may imply a negative attitude and malicious intent. Characteristics include

egotism, lack of empathy, lack of remorse, immorality and/or lack of ethics, impulsivity, and manipulation.[7, 26, 33]

In summary, these psychological elements could have consequences leading to insider threat in three main ways:

- Certain features of the Big Five model make individuals **more likely to disclose sensitive information**, **engage in unsafe behaviours/risk taking or fall victim to social engineering**. Agreeableness, for example, could influence a person's susceptibility to social engineering attacks, as these individuals are more trusting, generally altruistic, and compliant.[31]

- These psychological factors can lead to disruptive emotions/feelings that can cause individuals to be **less attentive and thus more prone to making mistakes** that constitute insider threat behaviours/situations. For example, a negative affect causes all sorts of disturbing moods that, in turn, cause stress and anxiety, which are ultimately expressed by a lack of attention.[19, 23, 29, 34, 35]

- **Certain personality traits make it easier to develop a negative frame of mind** and/or mistrust in the company, causing hostility, contempt of authority, discontent, feelings of superiority, lack of empathy or lack of remorse.[5, 26] For example, having a low score in the agreeableness dimension may point to psychological characteristics of hostility and discontent.[15] These individuals are thus more likely to engage in deliberate behaviour that's harmful to their company.

However, when dealing with psychological factors, it's important to keep in mind that these are individual characteristics that involve different reactions and behaviours depending on the individual and, more notably, on their environment and other external influences. These factors should therefore be viewed as psychological predispositions to possible insider threat behaviour rather than actual risk predictors that need to be addressed.

### Life course

Several characteristics related to an individual's personal trajectory have been identified as influencing the potential for insider threat:

- **Life events**: **Certain negative experiences may impact a person's psychological and/or physical state**, such as having a criminal record, losing a job, undergoing a major life change (for example, divorce or loss of a loved one), or suffering from physical and/or mental health problems.[7, 11, 36, 37] It should be noted, however, that **certain positive events may influence an individual's personality traits**, making them more or less likely to engage in insider threat behaviours. For example, obtaining a position with more responsibility may incite an individual to be more conscientious, making them less prone to committing errors.[38]

- **Attitudes and behaviours related to personal life** such as substance abuse or gambling.[7, 11, 15, 39]

- **Financial status and related concerns**.[5, 7, 11, 15, 29]

These elements of an individual's personal life can pose an insider threat risk in two ways:

- Because of an altered or weakened physical and/or psychological state, all these characteristics, including negative life events, **can have a high emotional impact and result in a range of disruptive effects, such as stress, anxiety, fear and fatigue.**[11, 40] This can make individuals less attentive and thus more prone to mistakes that lead to insider threat situations. For example, they may be more vulnerable to social engineering.[41]

- Certain life events can lead individuals to consider actions and behaviours that might harm their company. For example, individuals in financial distress may consider stealing

confidential information from their company and reselling it to improve their situation.[42, 43]

## Current issues

Despite various insider threat studies, including the identification of risk factors and their observable behaviours, there remain many areas of uncertainty that complicate preventive interventions. Therefore, when implementing such measures, companies should pay attention to the following:

- **It's extremely difficult to define the precursor events (risk factors) of an insider attack and thus to develop a detection model that integrates the observable behaviours (indicators) that might reveal these causes**. These risk factors and their indicators can indeed be quite diverse and affect individuals in very different ways, depending on their personal characteristics and ways of reacting.[6, 21, 27] It seems therefore complicated to develop instruments capable of objectively identifying and measuring the entire range of factors and their indicators.[6, 44]

- When taking stock of observable behaviours demonstrated in precursor events of an insider threat incident, **careful consideration should be given to legal and ethical issues, particularly respect for employee privacy**. Employees have a right to confidentiality that prohibits intrusion and the collection of information that could harm the individuals concerned. This means businesses can't simply gather any type of information they please on their employees to be used for any and all purposes.[35, 44] Furthermore, even if permitted, this type of information gathering **can create a permanent climate of surveillance and suspicion, as well as adversely affect employee satisfaction with their work or workplace relationships.**[44, 45] This could have the opposite effect of what was intended, actually heightening the risk of insider threat due to the emergence of negative attitudes among employees toward the company, such as disengagement and discontent. It could also cause disturbing feelings/emotions, such as stress or frustration, which in turn lead to mistakes.[11, 46]

- **It may be risky to encourage employees to report suspicious behaviours of colleagues that may indicate an insider threat.**[47] Besides the predictive difficulties outlined above, judgments and highly subjective interpretations by individuals of observed behaviours may interfere with preventive efforts.[14, 48] For example, it can **lead to a high number of false positives**, which could contribute to a widespread sense of suspicion, an atmosphere of denunciation and the deterioration of the work environment.

## Practical recommendations

Despite the issues identified above, the range of elements explored indicates that companies can implement measures to prevent insider threat, at least to a certain extent. As such, the following recommendations may be useful:

- **Raise awareness and train employees and managers to recognize signs of a potential risk situation.**[3, 5, 8, 21, 32] The goal is to heighten their awareness of organizational contexts that are conducive to insider threat and not for them to report their colleagues based on their personal characteristics. Moreover, sensitizing/training employees on current cybercrime attacks and how they're perpetrated will increase their awareness of the dangers they may face.

- Along with the knowledge of insider threat risk factors, it would be wise **to implement strategies to mitigate these risks**, for example

by improving working conditions or introducing unambiguous security regulations and instructions.[34] This could take the form of memos to all employees or posters on company premises clearly indicating acceptable and unacceptable behaviours to avoid leaving room for interpretation by employees of what they are and aren't allowed to do.[25] Task management and planning practices that respect employee capabilities could also be put in place to reduce the risk of stress due to the pressure to accomplish said tasks.[34] Another idea involves regularly checking and updating security systems and solutions as cybercrime techniques evolve.[49]

- **Create a database for identifying signs (indicators) to detect and track situations of concern**. To avoid false positives, this initiative must be based on objective data on known potential indicators of such situations, such as job changes or disciplinary action.[21] Also, to maintain confidentiality, it shouldn't be based on employees' personal data but rather on organizational data, specifically that related to the work environment and employee activities. This would require consent, but also and most importantly, clear communication with all employees on what data can be monitored and collected, why and for what purpose. In addition to addressing the legal aspect of data confidentiality, this would help employees understand the value of certain types of monitoring.[3, 45]

- **Exercise caution in the use of personal characteristics, such as psychological factors or employee life situations that don't, on their own, make it possible to identify cases of insider threat**. The individuals responsible for these situations have highly variable profiles, and the factors that cause these incidents often involve a combination of cognitive processes and factors that are triggered by situational elements. Thus, it would seem more relevant to try to limit the organizational factors that might favour this type of threat (see Part 1) and put in place opportunities for individuals with at-risk profiles to seek emotional, organizational and/or psychological support.[45, 50] These personal factors should perhaps be taken into account at the pre-employment investigation stage, during which the individual's career path, credit situation or personality may be assessed.[25]

## References

[1] Greitzer, F. L. (2019, April). Insider Threats: It's the HUMAN, Stupid! In Proceedings of the Northwest Cybersecurity Symposium (pp. 1–8).

[2] Magazine, C. S. O. (2011). US Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University, Deloitte: 2011 Cybersecurity Watch Survey. CSO Magazine.

[3] Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T. & Rogers, S. (2005). Insider threat study: Computer system sabotage in critical infrastructure sectors. National Threat Assessment Center, Washington DC.

[4] Ponemon Institute. (2020). 2020 Cost of Insider Threats Global Report.

[5] Dupuis, M. & Khadeer, S. (2016, September). Curiosity killed the organization: A psychological comparison between malicious and non-malicious insiders and the insider threat. In Proceedings of the 5th Annual Conference on Research in Information Technology (pp. 35–40).

[6] Greitzer, F., Purl, J., Leong, Y. M. & Becker, D. S. (2018, May). Sofit: Sociotechnical and organizational factors for insider threat. In 2018 IEEE Security and Privacy Workshops (SPW) (pp. 197–206). IEEE.

[7] Centre for the Protection of National Infrastructure. (2010). Ongoing Personnel Security: A Good Practice Guide.

[8] Elmrabit, N., Yang, S. H. & Yang, L. (2015, September). Insider threats in information security categories and approaches. In 2015 21st International Conference on Automation and Computing (ICAC) (pp. 1–6). IEEE.

[9] Leka, S., Griffiths, A., Cox, T. & World Health Organization. (2003). Work organisation and stress: systematic problem approaches for employers, managers and trade union representatives. Switzerland: World Health Organization.

[10] Pond, D. J. & K. R. Leifheit. (2003). End of an error. Security Management, 47(5). 113–117.

[11] Shaw, E. D. & L. F. Fischer. (2005). Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders. Report 1—Overview and General Observations. Technical Report 05-04, April 2005. Monterey, CA: Defense Personnel Security Research Center.

[12] Whitten, A. & J. D. Tygar. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, Washington, DC.

[13] Venkatesh, V., M. Morris, G. B. Davis & F. D. Davis. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478.

[14] M.R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, A. Moore, Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. In U.S. Secret Service and CERT® Coordination Center/SEI, 2005, p. 25.

[15] Shaw, E. D. & L. Sellers. (2015). Application of the critical-path method to evaluate insider risks. Studies in Intelligence, 59(2), 41–48.

[16] Costa, D. L., M. J. Albrethsen, M. L. Collins, S. J. Perl, G. J. Silowash & D. L. Spooner. (2016). An Insider Threat Indicator Ontology. Pittsburgh, PA: TECHNICAL REPORT CMU/SEI-2016-TR-007.

[17] Lehner, P., M. Seyed-Solorforough, M. F. O'Connor, S. Sak & T. Mullin. (1997). Cognitive biases and time stress in team decision making. IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems & Humans, 27, 698–703.

[18] Soetens, E., J. Hueting & F.Wauters. (1992). Traces of fatigue in an attention task. Bulletin of the Psychonomic Society, 30, 97–100.

[19] M.D. Rodgers, R.H. Mogfor, and B. Strauch. (2000). Post Hoc Assessment of Situation Awareness in Air Traffic Control Incidents and Major Aircraft Accidents. In M.R. Endsley and D.J. Garland (ed.), Situation Awareness Analysis and Measurement. Lawrence Erlbaum Associates: Mahway, NJ.

[20] Endsley, M. R. (1999, November). Situation awareness and human error: Designing to support human performance. In Proceedings of the high consequence systems surety conference (pp. 2–9).

[21] Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C. & Hohimer, R. E. (2012, January). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In 2012 45th Hawaii International Conference on System Sciences (pp. 2392–2401). IEEE.

[22] Huey, M. B. & Wickens, C. D. (1993). Workload Transition: Implications for Individual and Team Performance. National Academy Press.

[23] Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576–586.

[24] APA Dictionary of Psychology. (2015). Organizational Culture.

[25] Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? Information security technical report, 14(4), 186–196.

[26] Grebitus, C., Lusk, J. L. & Nayga Jr, R. M. (2013). Explaining differences in real and hypothetical experimental auctions and choice experiments with personality. Journal of Economic Psychology, 36, 11–26.

[27] McBride, M., Carter, L. & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. RTI International-Institute for Homeland Security Solutions, 5(1), 1.

[28] Mount, M., Ilies, R. & Johnson, E. (2006). Relationship of personality traits and counterproductive work behaviors: The mediating effects of job satisfaction. Personnel Psychology, 59(3), 591–622.

[29] Parrish Jr, J. L., Bailey, J. L. & Courtney, J. F. (2009). A personality based model for determining susceptibility to phishing attacks. Little Rock: University of Arkansas, 285–296.

[30] Salgado, J. F. (2002). The Big Five personality dimensions and counterproductive behaviors. International journal of selection and assessment, 10(1-2), 117–125.

[31] Weirich, D. & Sasse, M. A. (2001, September). Pretty good persuasion: a first step towards effective password security in the real world. In Proceedings of the 2001 workshop on New security paradigms (pp. 137–143).

[32] Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), 662–674.

[33] Shaw, E. D. & Stock, H. V. (2011). Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall. White Paper, Symantec, Mountain View, CA.

[34] Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D. & Cowley, J. (2014, May). Analysis of unintentional insider threats deriving from social engineering exploits. In 2014 IEEE Security and Privacy Workshops (pp. 236–250). IEEE.

[35] Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. & Whitty, M. (2014, May). Understanding insider threat: A framework for characterising attacks. In 2014 IEEE Security and Privacy Workshops (pp. 214–228). IEEE.

[36] Clark, L. A. & Watson, D. (1988). Mood and the mundane: Relations between daily life events and self-reported mood. Journal of personality and social psychology, 54(2), 296.

[37] Greitzer, F., Purl, J., Becker, D. E., Sticha, P. & Leong, Y. M. (2019, January). Modeling expert judgments of insider threat using ontology structure: Effects of individual indicator threat value and class membership. In Proceedings of the 52nd Hawaii International Conference on System Sciences.

[38] Srivastava, S., John, O., Gosling, S. & Potter, J. (2003). Development of Personality in Early and Middle Adulthood: Set Like Plaster or Persistent Change? Journal of Personality and Social Psychology, 1041–1053.

[39] Greitzer, F. L., Strozer, J., Cohen, S., Bergey, J., Cowley, J., Moore, A. & Mundie, D. (2014, January). Unintentional insider threat: contributing factors, observables, and mitigation strategies. In 2014 47th Hawaii International Conference on System Sciences (pp. 2025–2034). IEEE.

[40] Brown, S., Taylor, K. & Price, S. W. (2005). Debt and distress: Evaluating the psychological cost of credit. Journal of Economic Psychology, 26(5), 642–663.

[41] Gander, P., van den Berg, M. & Signal, L. (2008). Sleep and sleepiness of fishermen on rotating schedules. Chronobiology international, 25(2-3), 389–398.

[42] Lejuez, C. W., Aklin, W. M., Jones, H. A., Richards, J. B., Strong, D. R., Kahler, C. W. & Read, J. P. (2003). The balloon analogue risk task (BART) differentiates smokers and nonsmokers. Experimental and clinical psychopharmacology, 11(1), 26.

[43] Wang, L., Lu, W. & Malhotra, N. K. (2011). Demographics, attitude, personality and credit card features correlate with credit card debt: A view from China. Journal of economic psychology, 32(1), 179–193.

[44] Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R. & Ferryman, T. (2013). Psychosocial modeling of insider threat risk based on behavioral and word use analysis. e-Service Journal: A Journal of Electronic Services in the Public and Private Sectors, 9(1), 106–138.

[45] Greitzer, F. L. (2019, April). Insider Threats: It's the HUMAN, Stupid! In Proceedings of the Northwest Cybersecurity Symposium (pp. 1–8).

[46] Brown, W. S. (1996). Technology, workplace privacy and personhood. Journal of Business Ethics, 15(11), 1237–1248.

[47] Bell, A. J., Rogers, M. B. & Pearce, J. M. (2019). The insider threat: Behavioral indicators and factors influencing likelihood of intervention. International Journal of Critical Infrastructure Protection, 24, 166–176.

[48] D'Arcy, J., Hovav, A. & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information systems research, 20(1), 79–98.

[49] Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider. In Psychological and behavioral examinations in cyber security (pp. 46–63). IGI Global.

[50] Team, C. I. T. (2013). Unintentional insider threats: A foundational study. Research notebook CMU/SEI-2013-TN-022, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 18.

51 It should be noted that this table includes both risk factors and indicators of these causes because some are directly observable in the workplace and reflect a potentially risky situation..

## Appendix: Observable potential indicators of insider threat (non-exhaustive list)

| Psychological | Behavioural | Related to personal circumstances |
|---|---|---|
| Fatigue | Signs of discontent | Signs of radical thinking |
| Impulsivity | Signs of disengagement | Suspicious travel |
| Stress/anxiety | Disciplinary action | Recent negative events |
| Discontent | Difficulty accepting authority/criticism | Gambling |
| Mental health issues | Violation of company security rules | Substance abuse |
| Immorality/poor ethics | Poor work performance | Significant change in financial situation |
| Emotional instability | Recurring tardiness/absenteeism | |
| Anger management issues | Relationship issues with colleagues | |