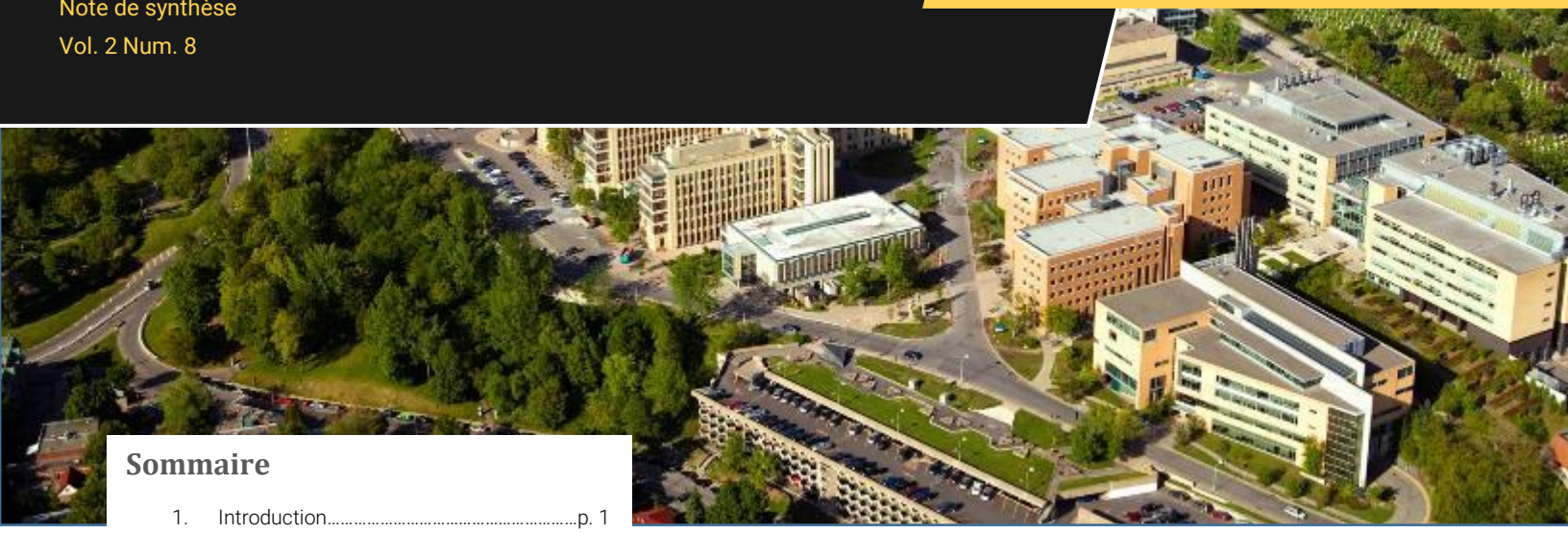
Les facteurs de risque de la menace interne

Adeline Veyrinas, M. Sc.

Note de synthèse
Vol. 2 Num. 8

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Introduction

La menace interne représente les « **menaces posées par des individus qui, intentionnellement ou non intentionnellement, détruisent, exfiltrent ou divulguent des informations sensibles, ou exposent leur organisation à des attaques extérieures** »[1]. Ce sont donc des individus qui, par leur comportement, nuisent à leur entreprise. Ces incidents, dont la fréquence est en augmentation, représenteraient **la deuxième plus grande menace en cybersécurité**, après le piratage externe. Ils seraient également les plus coûteux pour les organisations[2, 3]. Ainsi, en deux ans, le nombre d'incidents liés à des cas de menace interne a augmenté de 47% et leur coût pour les entreprises de 31%[4]. Cela concerne aussi bien les coûts directs liés à un incident tels que les pertes financières, d'exploitation ou réputationnelles, que les coûts indirects comme les frais juridiques de défense ou ceux de réparation des systèmes.

La menace interne intentionnelle peut s'exprimer via des actes aussi divers que l'espionnage, le sabotage, le détournement de fonds, l'extorsion ou encore la corruption[5, 6]. Lorsqu'elle est non intentionnelle, elle peut, par exemple, prendre la forme de la divulgation d'identifiants de connexion à la suite d'une attaque par ingénierie sociale ou d'une intrusion sur un équipement portable en raison d'une connexion à un réseau non sécurisé[5].

Ces menaces peuvent avoir d'importantes répercussions sur les entreprises,

comme des pertes financières majeures ou ternir leur réputation[7]. De ce fait et idéalement, elles devraient être gérées en amont, dans le cadre d'une stratégie de prévention. Cependant, cela représente une réelle problématique car il est souvent difficile d'identifier les causes et comportements annonciateurs d'une menace interne[1]. En effet, les comportements observables qui peuvent indiquer qu'un individu va représenter, ou non, une menace interne sont extrêmement variés et leur présence ne signifie pas nécessairement qu'il y aura effectivement une attaque interne. De plus, lorsque la menace interne est non intentionnelle, il semble difficile d'identifier des causes précises car il s'agit simplement d'erreurs qui ne sont donc pas nécessairement liées à des raisons ou motivations spécifiques. Cependant, les quelques études ayant été réalisées sur le sujet ont permis d'identifier certains facteurs de risque (causes de menace interne) dont la connaissance, en tenant compte de certains enjeux, permettrait de faire ressortir des recommandations pratiques pouvant être mises en place par les entreprises.

Facteurs de risque organisationnels

Environnement de travail

Plusieurs facteurs de risque liés à l'environnement de travail de l'entreprise ont été identifiés comme pouvant être des causes de menace interne. Les plus importants sont les suivants :

- Les politiques/procédures de sécurité : leur manque de clarté, leur communication inefficace aux employés et leur inadaptation aux conditions de travail freinent l'adoption de comportements sécuritaires[6, 8, 9, 10, 11, 12];
- Les outils technologiques : les difficultés d'utilisation, l'inadaptation des outils technologiques aux tâches des employés et le manque de sécurité dans la conception même de ces outils accentuent les risques [9, 10, 12] ;
- L'environnement direct : le bruit, la température, les conflits interpersonnels, l'ergonomie des installations bureautiques du milieu de travail peuvent aussi influencer la menace interne[10, 14, 15];
- Les pratiques managériales: le nombre de tâches à effectuer et/ou la pression élevée pour les réaliser, la mauvaise communication entre gestionnaires et employés, l'inadéquation entre les exigences des tâches et les connaissances et capacités des employés pour les accomplir peuvent enfin jouer un rôle significatif[6,8, 9,10,14,16, 17, 18].

L'ensemble de ces éléments peut entraîner des situations à risque de menace interne de deux manières :

- Les problématiques liées aux outils technologiques et aux règlements en matière de sécurité peuvent donner lieu à des comportements non sécuritaires ou à des prises de décision inadéquates, par exemple le fait de ne pas se servir d'outils trop difficiles à utiliser ou ne pas avoir connaissances des comportements à adopter[12, 13, 19];
- L'ensemble de ces facteurs de risque peut entraîner des émotions ou des sentiments perturbants, comme du surmenage, du stress, de l'anxiété ou de la fatigue. Cela peut alors affecter la performance des employés concernés et/ou les amener à commettre des erreurs, les rendant ainsi plus susceptibles d'être victime d'ingénierie sociale[9, 10, 17, 18, 19, 20, 21, 22, 23]. Cela peut également faire ressortir des émotions/sentiments qui relèvent du mécontentement ou de l'insatisfaction et qui peuvent affecter leur moral et l'état d'esprit vis-à-vis de leur employeur. Ils pourraient alors délibérément adopter des comportements allant à l'encontre du bien-être de l'entreprise[3, 6].

Culture d'entreprise

La culture d'entreprise incarne « un mode de pensée et de comportement distinctif, partagé par

les membres d'une même organisation et qui se reflète dans leur langage, leurs valeurs, leurs attitudes, leurs croyances et leurs coutumes »[24]. Deux situations peuvent représenter un risque de menace interne :

- La culture organisationnelle : dans le cadre d'un changement important dans la structure et/ou la gestion de l'entreprise, la transition peut être réalisée de manière brusque. Par exemple, une nouvelle direction ayant une vision différente de la sécurité peut instaurer une organisation et des procédures nouvelles sans tenir compte de la culture organisationnelle déjà en place ;

- La culture régionale : dans le cas où l'organisation possède différentes succursales situées dans des régions différentes, les règles, modes de gestion, conditions de travail ou directives de l'entreprise peuvent être différentes et entrer en conflit avec la culture des employés locaux. Également, les différences de langue entraînent parfois des perceptions et interprétations différentes de ce qui est communiqué en fonction de la culture de chacun[25].

Ces problématiques liées à la culture de l'entreprise peuvent entraîner différentes situations de menace interne :

- Affects émotionnels, comme la peur, l'incertitude ou les doutes qui peuvent rendre les individus plus susceptibles de commettre des erreurs et d'être ainsi victime d'ingénierie sociale[21, 25] ;

- Tensions entre les employés et leur entreprise avec des sentiments de manque de reconnaissance ou de négligence, ce qui peut entraîner une plus grande susceptibilité aux erreurs et/ou aux états d'esprit négatifs vis-à-vis de l'organisation[11, 21, 26];

- En plus des tensions qui peuvent apparaître, les employés peuvent souffrir d'un manque d'identification qui peut conduire au désengagement et à l'indifférence envers leur entreprise[5]. Cela peut alors entraîner les individus concernés à délibérément adopter des comportements allant à l'encontre du bien-être de leur entreprise[25].

Facteurs de risque individuels

Facteurs psychologiques

Parmi les facteurs psychologiques pouvant affecter négativement les employés d'une entreprise, il existe trois grandes catégories :

- Le modèle des BIG FIVE : ce modèle définit la personnalité d'un individu selon cinq grandes dimensions prévalentes. Il comprend : l'ouverture (ouverture à l'expérience), la conscienciosité (ordre, discipline, organisation), l'extraversion (énergie, émotions positives), l'agréabilité (sociabilité, bienveillance) et le neuroticisme ou névrosisme (instabilité émotionnelle, émotions négatives). Certaines dimensions de ce modèle ont été clairement identifiées comme pouvant jouer un rôle dans le développement de la menace interne, notamment l'agréabilité, le neuroticisme, l'ouverture et l'extraversion lorsque ceux-ci sont positifs (c'est-à-dire que plus l'individu présente ce trait, plus il est à risque), et le caractère consciencieux lorsque négatif (c'est-à-dire que moins l'individu présente ce trait, plus il est à risque)[5, 7, 27, 28, 29, 30, 31]. Cependant, l'implication des différentes dimensions dans les cas de menace interne reste à vérifier pour certaines et diffère en fonction des individus et du type de menace en question. Si l'agréabilité et la conscienciosité ont fait leurs preuves dans les cas de menace interne avérés, a contrario, le neuroticisme peut être un facteur d'absence de menace interne lorsqu'il implique une anxiété liée à l'ordinateur et donc une utilisation moindre des technologiques en réseau[29]. De plus, ces dimensions ne sont pas immuables et certains évènements de la vie d'un individu peuvent les

influencer dans un sens ou un autre, et ainsi peser sur le risque de menace interne. Par exemple, des antécédents de victimisation dans le cadre d'une escroquerie influenceraient négativement la dimension de l'agréabilité et donc la susceptibilité de victimisation à de l'ingénierie sociale[32];

- **L'affect** : il représente les types d'émotions que peuvent ressentir les individus et les différentes humeurs qui y sont liées. Ainsi, certains traits de l'affect, notamment négatifs, ont été identifiés comme jouant un certain rôle dans l'apparition de comportements et/ou circonstances de menace interne, tels que l'appropriation d'un bien de l'entreprise sans autorisation, l'utilisation de drogues/alcool sur le lieu de travail ou l'absentéisme[28]. Les affects recensés dans ces cas sont généralement l'hostilité, la tristesse, la peur, la faible estime de soi, la timidité ou encore l'inattention[5, 7];

- **La Triade noire** : elle représente trois traits de personnalité, à savoir **le narcissisme** (mégalomanie, égoïsme), **le machiavélisme** (manipulation, immoralité) et **la psychopathie** (impulsivité, manque d'empathie) pouvant impliquer une attitude négative et une intention malveillante. C'est le cas de l'égoïsme, du manque d'empathie, du manque de remords, du sens immoral et/ou non éthique, de l'impulsivité ou encore de la manipulation[7, 26, 33].

En résumé, ces éléments psychologiques pourraient avoir des conséquences impliquant la présence d'une menace interne de trois grandes manières :

- Certains traits du modèle des BIG FIVE rendent les individus **plus susceptibles de divulguer des informations sensibles**, **d'adopter des comportements non sécuritaires/de prise de risque ou d'être victimes d'ingénierie sociale**. Par exemple, l'agréabilité aurait une certaine influence dans la susceptibilité d'être victime d'attaque par ingénierie sociale parce que les individus font facilement confiance, sont plus généralement altruistes et de se conforment aux règles[31];

- L'ensemble de ces facteurs psychologiques peut entraîner des émotions/sentiments perturbateurs pouvant mener les individus à être **moins attentifs et ainsi commettre des erreurs** représentant des comportements/situations de menace interne. Par exemple, l'affect négatif entraîne toute sorte d'humeurs perturbantes pouvant causer du stress et de l'anxiété, se manifestant ainsi en un manque d'attention[19, 23, 29, 34, 35];

- **Certains traits de personnalité rendent plus facile l'apparition d'un état d'esprit négatif** et/ou de méfiance envers l'entreprise, comme l'hostilité, le mépris de l'autorité, le mécontentement, le sentiment de supériorité, le manque d'empathie ou le manque de remords[5, 26]. Par exemple, avoir un score peu élevé dans la dimension de l'agréabilité peut être révélateur de caractéristiques psychologiques d'hostilité et de mécontentement[15]. Cela rend ainsi les individus plus susceptibles de s'engager délibérément dans des comportements nuisibles à leur entreprise.

Toutefois, lorsqu'il s'agit de facteurs psychologiques, il est important de garder à l'esprit qu'il s'agit de caractéristiques individuelles qui impliquent des réactions et des comportements différents selon les individus, notamment en fonction de leur environnement et autres influences extérieures. Ces facteurs doivent donc être considérés davantage comme des prédispositions psychologiques à la possibilité d'un comportement de menace interne que comme de réels facteurs prédicteurs du risque sur lesquels il convient d'intervenir.

Parcours de vie

Plusieurs caractéristiques liées à la trajectoire personnelle d'un individu ont été identifiées comme pouvant avoir une certaine influence sur la

possibilité que celui-ci représente une menace interne :

- **Les évènements de vie** : **certaines expériences négatives peuvent avoir des conséquences sur l'état psychologique et/ou physique des individus** concernés, comme le fait de posséder un casier judiciaire, de perdre un emploi, de subir un changement de vie majeur (divorce ou perte d'un être proche, par exemple), ou encore de présenter des problématiques de santé physique et/ou mentale[7, 11, 36, 37]. À noter, toutefois, que **certains évènements positifs peuvent influencer les traits de personnalité** d'un individu et ainsi le rendre plus ou moins susceptible d'adopter des comportements de menace interne. Par exemple, le fait d'obtenir un poste avec plus de responsabilités peut pousser l'individu concerné à renforcer sa conscienciosité, et donc le rendre moins sujet au fait de commettre des erreurs[38];

- **Les attitudes et comportements liés à la vie personnelle** des individus, comme l'abus d'alcool/drogue ou le jeu[7, 11, 15, 39];

- **Le statut financier et les préoccupations attenantes**[5, 7, 11, 15, 29].

Ces éléments de la vie personnelle des individus peuvent représenter un risque de menace interne de deux manières :

- Du fait d'un état physique et/ou psychologique altéré ou affaibli, l'ensemble de ces caractéristiques, notamment les évènements de vie négatifs, **peut avoir un fort impact émotionnel et entraîner toute sortes d'affects perturbateurs, comme le stress, l'anxiété, la peur ou encore la fatigue**[11, 40]. Cela peut alors amener les individus concernés à être moins attentifs et ainsi commettre des erreurs menant à des situations de menace interne, par exemple les rendre plus vulnérables à de l'ingénierie sociale[41];

- Certains évènements de vie peuvent entraîner les individus à envisager des actions et adopter des comportements qui pourraient nuire à leur entreprise. Par exemple, les individus en situation de détresse financière, peuvent envisager de voler des informations confidentielles à leur entreprise pour les revendre afin de remédier à leur situation[42, 43].

Enjeux actuels

Malgré les différentes études menées en matière de menace interne, notamment sur l'identification des facteurs de risque et leurs comportements observables, il reste de nombreuses zones d'incertitude qui compliquent les interventions préventives. Ainsi, lorsqu'elles souhaitent mettre en place de telles mesures, les entreprises devraient prêter attention aux éléments suivants :

- **Il est extrêmement difficile de définir les évènements précurseurs (facteurs de risque) d'une attaque interne et ainsi de développer un modèle de détection qui intègre les comportements observables (indicateurs) révélateurs de ces causes**. En effet, ces facteurs de risque et leurs indicateurs peuvent être très divers et impliquer les individus de manières très différentes, en fonction de leurs caractéristiques personnelles et de leurs façons de réagir[6, 21, 27]. Il paraît alors compliqué de développer des instruments capables de recenser et mesurer de manière objective l'ensemble de ces facteurs et leurs indicateurs [6, 44];

- Lorsqu'il s'agit de collecter les comportements observables des évènements précurseurs d'un incident relié à la menace interne, il convient de **soigneusement considérer les questions légales et éthiques, et tout particulièrement le respect de la vie privée des employés**. En effet, il existe un droit à la confidentialité impliquant l'interdiction d'intrusion et de collecte d'informations susceptibles de nuire aux individus concernés. Cela empêche ainsi les entreprises de récolter

n'importe quel type d'informations sur leurs employés et de s'en servir dans n'importe quel but[35, 44]. De plus, même si cela est autorisé, ce type de collecte d'informations **peut susciter un climat de surveillance et de suspicion permanent, tout comme cela peut nuire à la satisfaction des employés quant à leur travail ou leurs relations à l'interne**[44, 45]. Cette situation pourrait créer l'effet inverse à celui recherché et alors représenter un risque de menace interne avec l'apparition, chez les employés, d'un état d'esprit négatif envers leur entreprise, comme un désengagement ou du mécontentement. Également, cela pourrait donner lieu à des émotions/sentiments de perturbation, comme le stress ou la frustration, entraînant ainsi des erreurs[11, 46];

- **Il semble hasardeux d'inciter les employés à signaler les comportements suspects de collègues qui pourraient être révélateurs d'une menace interne**[47]. Outre les difficultés prédictives soulignées plus haut, les jugements et les interprétations très subjectifs de chacun quant aux comportements observés peuvent venir interférer avec les efforts de prévention[14, 48]. Par exemple, cela peut **générer un nombre élevé de faux positifs**, ce qui pourrait contribuer à la diffusion d'un sentiment de suspicion et de délation généralisé et à la détérioration du climat de travail.

Recommandations pratiques

Malgré les problématiques relevées plus haut, il ressort de l'ensemble des éléments explorés qu'il est possible pour les entreprises, dans une certaine mesure, de mettre en place des mesures de prévention de la menace interne. Ainsi, les recommandations suivantes peuvent être utiles :

- **Sensibilisation et formation des employés et des gestionnaires afin de reconnaître les signes révélateurs d'une possible situation à risque**[3, 5, 8, 21, 32]. L'objectif est de les sensibiliser à un contexte organisationnel qui favorise l'établissement d'une menace interne et non de dénoncer leurs collègues sur la base des caractéristiques personnelles de ces derniers. Également, la sensibilisation/formation des employés sur les attaques de cybercriminalité actuelles et les moyens par lesquels elles sont perpétrées augmenterait leur prise de conscience des dangers auxquels ils peuvent être confrontés ;

- Avec la connaissance des facteurs de risque de menace interne, il serait approprié de **mettre en place des stratégies d'atténuation de ces risques**, par exemple via l'amélioration des conditions de travail ou l'instauration de règlements et d'instructions non-équivoques en matière de sécurité[34]. Cela pourrait prendre la forme de notes diffusées à l'ensemble des employés ou d'affiches dans les locaux de l'entreprise indiquant clairement les comportements acceptables et non acceptables pour éviter de laisser place à l'interprétation des employés sur ce qu'ils peuvent faire ou ne pas faire[25]. Il pourrait également être mis en place une gestion et une planification des tâches respectueuses de la capacité des employés afin de réduire les risques de stress dû à la pression induite par la réalisation de ces tâches[34]. Une autre idée pourrait être de vérifier et mettre régulièrement à jour les systèmes et solutions de sécurité en fonction de l'évolution de la cybercriminalité et des techniques utilisées par les cybercriminels[49];

- **Création d'une base de données permettant de recenser les signaux (indicateurs) pour repérer et suivre les situations préoccupantes**. Pour éviter les problèmes de faux positifs, cette initiative doit s'appuyer sur des données objectives qui seraient de potentiels indicateurs d'une telle situation, comme le changement de poste ou les actions disciplinaires reçues[21]. Également, afin de ne pas menacer la confidentialité des données, il convient de se baser sur des données organisationnelles et non pas sur les données personnelles des employés, donc ce qui est lié

à l'environnement et au contexte de travail et aux activités des employés. Il faudrait alors obtenir leur consentement, mais aussi et surtout communiquer clairement avec tous les employés sur les données qui peuvent être surveillées et collectées, dans quel but et pourquoi. En plus de répondre à l'aspect légal sur la confidentialité des données, cela permettrait de faire comprendre aux employés l'intérêt de certains types de surveillance[3, 45];

- **Prudence face à l'usage des caractéristiques personnelles, telles que les facteurs psychologiques ou la situation de vie des employés, qui ne permettent pas, à eux seuls, d'identifier les cas de menace interne**. Les profils des individus responsables de ces situations sont très variables et les facteurs à l'origine de ces incidents impliquent souvent une combinaison de processus et facteurs cognitifs qui sont déclenchés par des éléments situationnels. Ainsi, il semblerait plus pertinent d'essayer de limiter principalement les facteurs organisationnels qui pourraient favoriser ce type de menaces (cf. partie 1) et de mettre en place la possibilité d'un soutien émotionnel, organisationnel et/ou psychologique pour les personnes présentant des profils à risque[45, 50]. Il convient alors d'éventuellement prendre en compte ces facteurs personnels au stade de l'enquête de pré-emploi, que ce soit le parcours professionnel, la situation de crédit ou de la personnalité des individus concernés[25].

Références

[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 Insistute 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 Ctr 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, D.C.

[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, pp. 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 ofr 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. cahier de recherche CMU/SEI-2013-TN-022, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 18.

51 A noter que ce tableau regroupe aussi bien des facteurs de risque que des indicateurs de ces causes car certaines sont directement observables sur le lieu de travail et révélatrices d’une situation potentiellement à risque.

Annexe. Indicateurs observables potentiellement révélateurs d'une menace interne (liste non exhaustive)

Psychologiques	Comportementaux	Liés à la situation personnelle
Fatigue	Signes de mécontentement	Signes de pensée radicale
Impulsivité	Signes de désengagement	Voyages suspects
Stress/anxiété	Mesures disciplinaires reçues	Récents évènements négatifs
Mécontentement	Difficultés d'acceptation de l'autorité/critique	Jouer à des jeux d'argent
Problèmes de santé mentale	Violation des règles de sécurité de l'entreprise	Abus d'alcool/drogues
Immoralité/faible sens éthique	Faible performance de travail	Changement significatif dans la situation financière
Instabilité émotionnelle	Retards répétitifs/absentéisme	
Problèmes de gestion de la colère	Problèmes relationnels avec les collègues	