Integrating quantitative and qualitative reasoning to mitigate threats

Received (in revised form): 2nd December, 2025

Frank L. Greitzer
Chief Behavioural Scientist, Cogility Software, USA

Frank Greitzer is the Chief Behavioural Scientist for Cogility Software, where he supports development and deployment of advanced decision intelligence solutions including predictive models for insider risk management. Frank is also the owner and Principal Scientist of PsyberAnalytix, which he founded in 2012 to perform research and consulting in social/behavioural sciences and information security. Prior to this, he served as Chief Scientist in cognitive informatics at the US Department of Energy's Pacific Northwest National Laboratory. In Frank's early career, after earning a BSc degree in mathematics from Harvey Mudd College, Claremont CA, USA, a MA degree in psychology and a PhD in mathematical psychology from UCLA, Los Angeles CA, USA, he served as a research psychologist for the US Navy and a human factors and artificial intelligence (AI) researcher in the aerospace industry. Among Frank's most notable recent achievements is the development of a comprehensive knowledge base of behavioural and technical insider risk indicators. His contributions to research and practice also include numerous journal articles, conference papers and invited talks.

Cogility Software, 15495 Sand Canyon Ave, Suite 150, Irvine, CA 92618, USA
Tel: +1 509 539 4250; E-mail: fgreitzer@cogility.com

Abstract Traditional threat assessment approaches used by insider threat hubs and law enforcement are primarily reactive, focusing on the response to an incident and collecting forensic data to support the investigation. More mature, proactive programmes aim to prevent or mitigate risks with specialised behavioural threat assessment analysts, who use multidisciplinary approaches to identify and manage at-risk individuals before an incident occurs. Threat assessment methods range from the use of individual, unstructured clinical judgments to formal qualitative models that provide structured guidelines, to predictive analytic models. This paper describes the aims and characteristics of qualitative and quantitative models to anticipate insider threats and discusses the integration of these traditionally divergent threat assessment methods, highlighting the importance of combining human judgment, data science and artificial intelligence (AI) to develop holistic risk management strategies. This article is also included in **The Business & Management Collection** which can be accessed at https://hstalks.com/business/.

KEYWORDS: behavioural threat assessment, insider threat, insider risk, structured professional judgment, violence risk assessment

DOI: 10.69554/MMVD9759

INTRODUCTION AND BACKGROUND

An insider threat is a security risk posed by individuals within an organisation, such as current or former employees or contractors, who misuse their authorised access to cause harm to sensitive data, systems or other organisational assets (including people). While cyber security threats such as malicious insider-initiated data breaches are perhaps the most recognisable insider risks — and arguably the most expensive to remediate — there is a variety of types of insider risk that include insider fraud, sabotage and workplace violence in addition to data exfiltration and unauthorised disclosures/breaches.[1]

Surveys and studies over the last two decades have reported an increasing trend in the occurrence of insider threat incidents. Cybersecurity Insiders' 2025 report[2] found that nearly half of organisations reported that insider attacks have become more frequent, and 29 per cent of respondents reported that the average cost of remediation exceeds US$1m. Similarly, incidents involving violence — whether associated with insider/workplace risk or with other forms of targeted violence in our communities — have increased in frequency and intensity over the past several decades.[3]

Importantly, a significant majority (77 per cent) of organisations polled, as stated in the Cybersecurity Insider report, lacked confidence in their ability to detect and mitigate insider threats, and 71 per cent identified lack of adequate tools and technologies as a major obstacle preventing their organisation from improving its insider threat management programme.[4] In addressing targeted violence, research focusing on radicalisation and violent extremism has not been systematically applied to develop and deploy tools designed for law enforcement or community practitioners.[5] Nevertheless, law enforcement is increasingly tasked with identifying and managing targeted violence risk.

Traditional threat assessment approaches used by insider threat hubs and law enforcement are primarily reactive, focusing on the response to an incident and collecting forensic data to support the investigation (and prosecution, if applicable). There is a need for proactive methods that can prevent or mitigate the risks. To this end, more mature programmes establish risk management teams composed of specialised behavioural threat assessment analysts, who employ multidisciplinary strategies to proactively identify and manage at-risk individuals (persons of concern [POC]) before incidents occur — as recommended by leading US Government stakeholders such as the National Insider Threat Task Force's Insider Threat Program Maturity Framework[6] and the Federal Bureau of Investigation's (FBI) report, 'Making Prevention a Reality'.[7]

Implementing this more proactive approach to risk assessment requires a paradigm shift that changes the focus of the analysis from gathering facts on the elements of a crime to the collection and assessment of behavioural/background information relevant to risk and contributing factors. Thought leaders in the insider threat research[8,9,10] and violence risk assessment[11,12] communities emphasise the need to proactively address behavioural factors associated with individuals who may be on a critical pathway leading towards an attack. These methods systematically evaluate behaviours or conditions that have been identified through behavioural science research as potential risk indicators. For insider risk, an exemplary knowledge base of insider risk indicators is the Sociotechnical and Organizational Factors for Insider Threat (SOFIT) taxonomy.[13] For violence risk assessment, the FBI Behavioral Analysis Unit's 2017 Report on 'Making Prevention a Reality'[14] provides an authoritative collection of behavioural indicators for targeted violence attacks.

In addition to the historical chasm between reactive methods focusing on

forensics and proactive approaches that examine behavioural factors, there has been an ongoing debate in the threat assessment community between those who advocate qualitative versus quantitative risk modelling approaches. This paper explores the roles of qualitative and quantitative models in supporting proactive insider threat assessment: their major features, advantages and limitations, and the potential for integrating these approaches to enhance decision-making processes.

QUALITATIVE MODELS

Qualitative models use descriptive, non-numerical constructs to represent processes or relationships. They incorporate expert opinions, contextual knowledge, experience and subjective factors to produce comparative predictions and causal hypotheses. These models are well suited for exploring complex phenomena and developing theories or hypotheses; however, they are limited by the potential influence of the researcher's perspective and biases, making it difficult to scientifically replicate findings.

Insider risk frameworks

Examples of qualitative models for insider risk are the SOFIT knowledge base of insider risk indicators[15] (see Figure 1[16]), and Eric Shaw's Critical Pathway to Insider Risk[17,18] (see Figure 2).

Originally developed in a project funded by IARPA in 2016–19, the SOFIT framework has been updated to provide a three-level hierarchy of potential risk indicators (PRIs). The individual factors branch[19] of SOFIT2.0 specifies nine major classes (boundary violations, security violations, job performance, financial concerns, foreign ties, criminal activities, ideology, psychological factors and cyber security factors), which are in turn divided into 33 subclasses (shown as grey boxes in Figure 1) that contain the individual factors, which comprise the third level of the SOFIT2.0 hierarchy with approximately 200 PRIs. In addition to specifying PRIs, SOFIT distinguishes among different threat behaviours of concern, including (but not limited to) exfiltration, fraud, sabotage, espionage, workplace violence and unintentional insider threat.

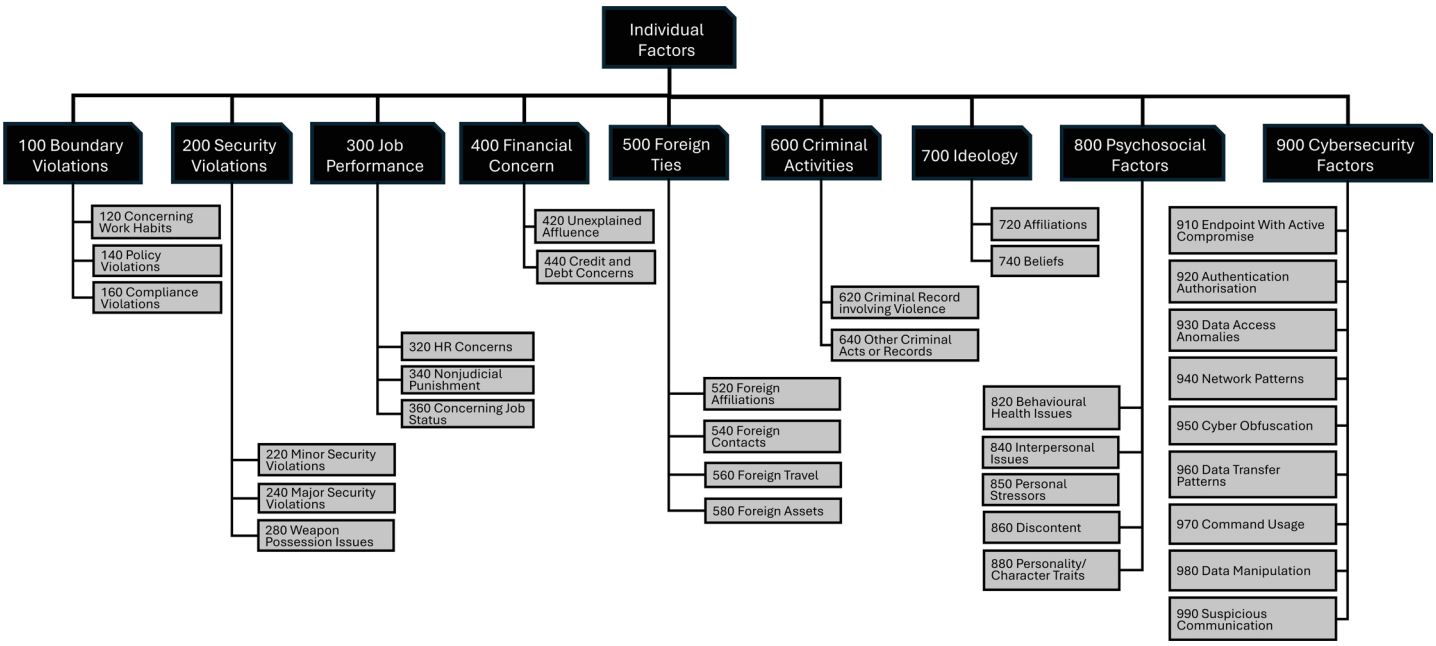

Figure 1: SOFIT framework for insider risk indicators — individual factors branch

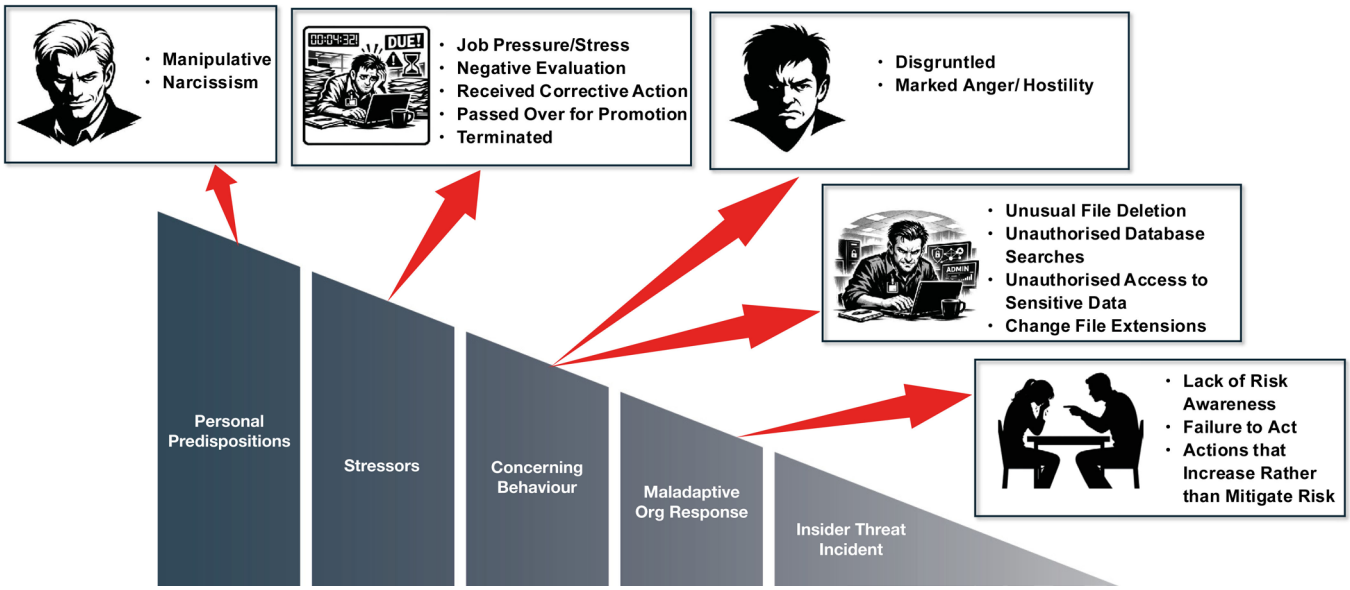

Figure 2: Depiction of Shaw's CPIR

Each individual PRI maps to (is associated with) one or more threat behaviour types. The strength of association between a given PRI and a specific threat behaviour is typically referred to as a 'weight'. PRI weights are determined through 'calibration' studies conducted with behavioral science and cybersecurity/information assurance experts. Analysts who use this knowledge base can readily modify the PRI weights and their mappings to threat behaviours. At the discretion of the insider risk management team, the SOFIT knowledge base with associated weights/mappings can be applied to inform the implementation of quantitative, predictive insider risk models.

The Critical Pathway to Insider Risk (CPIR) framework, developed by Eric Shaw and colleagues, reflects 'a strong pattern of subject risk factors and organizational behavior common across such insider offenses as espionage, sabotage, violent attacks on employees and parallel offenses such as theft of commercial intellectual property'.[20] The CPIR framework describes psychological vulnerabilities and risk factors such as personality traits, personal and professional stressors that trigger the underlying risk factors, and concerning behaviours that reflect violations of policies, rules or laws. The pathway also considers possible problematic management efforts in responding to these observed risks that exacerbate the problems by escalating instead of reducing the threat. In addition, the CPIR framework describes mitigating or protective factors that often prevent most individuals who are otherwise at risk from going on to commit insider incidents. Examples of protective factors are social support in relationships that help reduce stress, positive temperament that helps to provide stress resistance through coping abilities, and enlightened management that seeks wellness instead of punishment by providing resources and support through intervention/remediation options.[21]

Structured professional judgment approaches for violence risk assessment

Leading qualitative threat assessment models use structured professional judgment (SPJ) methods, which implement techniques that are informed by structured, evidence-based guidelines. SPJ tools promote consistent

decision making while incorporating expert insights. Most often deployed for violence risk assessment, SPJ tools foster a systematic, fact-based assessment of contributing factors that yields an overall risk judgment and a risk mitigation plan. SPJ techniques generally include the following steps (see Figure 3):

- Information gathering to determine the presence of risk and protective factors. Risk factors may correspond to many of the PRIs defined in insider risk indicator taxonomies such as SOFIT and may include observed behaviours that indicate planning, preparation or intent. Protective factors, as noted above, reflect attitudes, temperament or relationships that may help to reduce the impact of risk factors.
- Determining the relevance of these factors in assessing where the subject is on the pathway to insider threat. This includes linking the behaviours to possible threat/risk types.
- Risk formulation, to explain the available evidence and risk indicators and identify the most likely risks. This may include the development of narratives that describe possible risk scenarios.
- Risk management, focusing on development of mitigation strategies such as interventions and safety measures to reduce vulnerability of targets.
- Decision on final risk judgment, prescribing a risk management plan tied to the most likely risk scenario(s) and the associated degree of concern.

A widely used SPJ approach that focuses on workplace violence is the Workplace Assessment of Violence Risk (WAVR-21) tool, which defines 21 risk factors (see Table 1) that should be considered when assessing violence risk.[22] The structured process requires the analyst to examine the information about a case to determine whether each of these risk factors is present (where each indicator is determined to be 'not present', 'present' or 'prominent'). Given this collection of observed indicators, the analyst then considers the possible risk scenarios associated with these factors. The process yields a report that identifies possible strategies to mitigate the risks of these scenarios and provides a final risk judgment (eg an ordinal 'low–medium–high' rating of the analyst's degree of concern). The WAVR-21 tool is focused on workplace violence and is intended for use by mental health professionals.

In conducting violence risk assessments, it is important to collect information about environmental factors (eg family/work environment, mental health factors) in addition to concerning behaviours. While law enforcement professionals are well positioned to conduct *ex-post facto* investigations of criminal conduct, they are rarely trained to proactively gather information regarding behavioural indicators of future concerning conduct. The North Carolina Behavioral Threat Assessment (BeTA) Investigation Overview (NCBIO-25) tool provides evidence-based structure

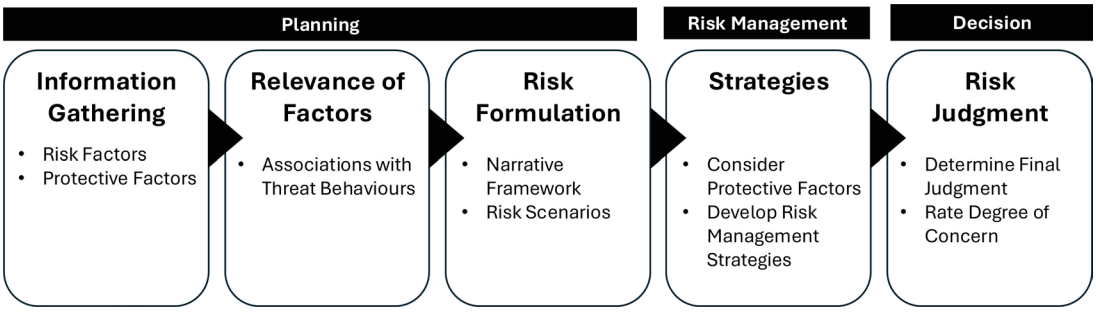

Figure 3: Steps in SPJ

Table 1: WAVR-21 workplace violence risk factors

• Motives for violence	• Anger problems
• Homicidal ideas, violent preoccupations or identifications	• Suicidality and/or depressive mood
• Threatening communications or expressed intent	• Irrationally suspicious or bizarre beliefs
• Weapons skill and/or access	• Substance abuse and/or dependence
• Pre-attack planning and preparation	• Increasing isolation
• Stalking or menacing behaviour	• History of violence, criminality and/or conflict
• Current job or academic problems	• Domestic/intimate partner violence (IPV)
• Extreme job or academic attachment	• Situational and organisational contributors to violence
• Loss, personal stressors and negative coping	• Stabilisers and buffers against violence
• Entitlement and other negative traits	• Organisational impact of real or perceived threats
• Lack of conscience and irresponsibility	

and guidance for law enforcement teams to use in conducting threat assessments.[23]

The NCBIO-25 tool is distinguished from other SPJ tools for violence risk assessment that require users to have advanced qualifications in a mental health profession, that are specialised for use in specific settings (such as workplace violence, school settings) or that are developed for use with specific populations (eg youth). The tool includes 25 risk variables organised into five categories or 'domains of interpretation': targeted threat risk, weapons, environmental risk, mental health risk, behavioural risk (see Table 2; based on Jones *et al.*[24]). For 19 of the items, raters may also score a relevant protective factor (these factors are identified with an asterisk in the table). In addition to the 25 primary factors, the methodology captures categorical information about identifiable grievance, deceptive indicators, cessation behaviours, ideographic risk or protective factors and overall impressions that may be relevant to case management.

As described in Jones *et al.*,[25] a preliminary investigation is conducted to collect behavioural evidence on whether the subject has the motive (grievance) and means (access to weapons) to carry out an attack of targeted violence, the immediacy of targeted violence risk, any immediate environmental circumstances and presence of any key external influencers. This initial assessment determines whether a full threat assessment is warranted. The full assessment is guided by the NCBIO-25 tool, culminating in the final risk assessment and mitigation strategies based on observable risk and protective factors.

The SPJ approach compares favourably to unstructured clinical judgment, in which the analyst uses their best judgment to evaluate which risk factors are relevant and the importance of those risk factors, without the aid of any formalised rubric or protocol.[26,27] Compared to unaided clinical judgment by mental health professionals, the SPJ approach yields greater consistency in output, particularly in the risk assessment phase of the analysis.[28] For example, Jones *et al.* reported high interrater reliability for the NCBIO-25 tool among raters trained in threat assessment, with intraclass correlation coefficient of 0.87.

QUANTITATIVE MODELS

Quantitative models generate numerical predictions of phenomena, facilitating empirical testing and validation. Predictive analytic models that represent a whole-person approach (including behavioural/psychosocial indicators in addition to cyber security data) and those that are explainable (rather than machine learning [ML] 'black box' approaches) are of primary concern here. These quantitative models develop formal representations of constructs and variables to describe the components of a system and how they interact, enabling more rigorous testing of model predictions of the system's behaviour.

Table 2: Summary of NCBIO-25 behavioural threat assessment factors

Risk factor	Description	Measurement scale
Targeted threat risk		
• Harming others	• Subject talks about harming others or carrying out an attack	Scored using a 4-point ordinal scale: 0 = not present 1 = ideation 2 = intent 3 = behavioural indicators present
• Threats • Leakage • Violent identity	• Subject communicates direct threat(s) • Subject communicates to a third party about threat behaviour • Subject becomes preoccupied or identifies with previous targeted attacks or attackers	Scored using a 3-point ordinal scale 0 = not present 1 = present 2 = present, elevated
Weapons		
• Weapons interest*	• Subject talks about guns or weapons and/or subject expresses interest in weapons for inappropriate use or reasons	Scored using a 3-point ordinal scale reflecting severity: 0 = not present 1 = present 2 = present, elevated
• Weapons access	• Subject has access to at least one firearm or other identifiable weapon of choice	Scored using a 3-point ordinal scale reflecting severity: 0 = no access/no prior firearms experience or training 1 = restricted weapons access/firearms use with no advanced training 2 = unrestricted weapons access/ advanced firearms training
• Weapons proficiency	• Subject's level of skills and training with identified weapon of choice	
Environmental risk		
• Home environment* • Family dynamics* • Social supports* • Financial* • Work* • School*	• Subject has a chaotic home environment • Subject is experiencing problems in family interaction • Social supports — subject is having relationship problems or has experienced a loss of previously positive social supports • Financial — subject (or subject's family, if adolescent) is having financial problems • Work — subject is having difficulty in the work environment • School — subject is having difficulty in the school environment	Scored using a 3-point ordinal scale reflecting severity: 0 = not present 1 = present 2 = present, elevated
Mental health risk		
• Self-harm* • Mental health*	• Subject has a history of self-harm behaviours or current engagement in self-harm behaviours • Subject exhibits behaviours consistent with or self-reports current or past treatment for mental health disorder	Scored using a 3-point ordinal scale reflecting severity: 0 = not present 1 = present 2 = present, elevated
• Suicide*	• Subject has a history of or current suicidal thoughts, statements, gestures, or attempts	Scored using a 4-point ordinal scale: 0 = not present 1 = ideation 2 = intent 3 = behavioural indicators present
Behavioural risk		
• Personal appearance* • Inappropriate reactions* • Externalisation* • Intimidation* • Anger* • Substance abuse* • Sociopathy* • Extremism* • Interpersonal traits*	• Subject has a change in personal habits or appearance • Subject's reactions are inappropriate for the situation • Subject blames others for problems • Subject bullies or intimidates others • Subject uses abusive language that is inappropriate for the situation or has uncontrolled angry outbursts • Subject is abusing alcohol or drugs or both • Subject has a history of abusing animals or setting fires • Subject has an interest in extremist and/or hate ideals or groups • Subject shows evidence of harmful interpersonal qualities	Scored using a 3-point ordinal scale reflecting severity: 0 = not present 1 = present 2 = present, elevated

*Both risk and protective indicators are associated with this item

Overview of quantitative modelling approaches

In the threat assessment domain, there has been ongoing rivalry between quantitative and qualitative approaches. Actuarial models have been offered as quantitative modelling alternatives to unaided/unstructured clinical judgments for violence risk assessment. Proponents argue that because actuarial instruments focus on statistical properties or averages in the target population, they are not subject to the limitations of human threat assessment professionals, who may have different experiences, cognitive abilities, resources or priorities that could potentially introduce biases. Qualitative risk assessment advocates, however, argue that dependence solely on actuarial statistics does not allow the analyst to take account of the particularity of individual cases or enable them to apply their insights and judgments based on a case's unique characteristics. Thus, the qualitative SPJ approach (described in the previous section) offers an alternative framework that addresses the limitations of both actuarial models and unstructured clinical judgment.

Actuarial models are not the only type of quantitative approach available for risk assessment, however. Several representative predictive analytic modelling approaches are briefly summarised here:

- *Risk score aggregation approaches*: Numerous behavioural analytic approaches to propagate risk scores have been described. Kandias *et al*.[29] developed an insider threat prediction model that implements a capability–motivation–opportunity (CMO) concept within a multi-stage risk assessment, accumulating numeric threat ratings to yield an overall risk score. Legg *et al*.[30] and Legg[31] describe an anomaly-based insider threat detection system that produces multiple anomaly scores for various features according to importance, resulting in an anomaly score matrix reflecting 16 features, with alerts generated for scores that exceed a threshold. Greitzer *et al*.[32] describe several modelling approaches, including a sum-of-risk model that adds risk scores for observed PRIs, with risk weights informed by the SOFIT framework.
- *Bayesian modelling of behavioural risk factors*: Greitzer *et al*.[33] developed a Bayesian network model focusing on a dozen psychosocial/behavioural indicators (eg disgruntlement, absenteeism, etc.). An initial study obtained expert judgments for 110 scenario cases with 1–5 PRIs described, with results informing the conditional probabilities of a Bayesian model. The model was tested in a subsequent study comparing its predictions with expert judgments from ten experts who assessed 24 cases. Axelrad *et al*.[34] developed a predictive model that used a set of 83 psychosocial indicators — including environmental (personal, job) stressors, personality traits, personal variables (affect, attitude) and past counterproductive behaviour — which were ranked and combined into a single risk score using a Bayesian network. More recently, Elmrabit *et al*.[35] developed a CMO-based Bayesian network model, incorporating a broad range of technical, human (behavioural) and organisational factors. Greitzer *et al*.[36] created a Bayesian network model incorporating approximately 200 individual PRIs defined in the SOFIT framework[37] and compared the performance of the Bayesian model with other risk-based models (such as the sum-of-risk model mentioned above). The Bayesian model performed slightly better than the sum-of-risk model.
- *AI expert system-based models*: Artificial intelligence (AI) expert systems are computer programs that use AI to mimic the decision-making ability of a human expert. They rely on a knowledge base, informed by experts and inference engine/logic to apply this knowledge in solving complex problems. The

Cogynt model is an example of an AI expert system approach that includes a quantitative model to propagate insider risk. Cogynt uses hierarchical complex event processing (HCEP) to identify relevant insider risk indicators based on the SOFIT taxonomy. HCEP is a pattern-based representation of expert knowledge that is, by design, a model of the expert's decision analysis process. The Cogynt platform continuously ingests behavioural and technical data, computing and propagating insider risk up through the hierarchy to produce behavioural profiles and risk scores for all threat behaviour types of concern.

Quantitative threat assessment models have been evaluated using a variety of methods and metrics. There are similar performance metrics to compare for the most recent work by Elmrabit[38] and by Greitzer *et al.*[39,40] Each of these studies tested the models against expert judgments of insider risk: the squared correlation coefficient between expert ratings and the model predictions served as a performance metric. The Elmrabit study reported a squared correlation of 0.87; lower *r*-squared values around 0.60 were obtained for the sum-of-risk and Bayesian models in the Greitzer *et al.*[41,42] studies.

More recently, model performance in predicting expert judgments for 59 hypothetical cases was compared for the sum-of-risk model and the Cogynt AI expert system-based model.[43] More rigorous evaluations were performed using the *F1* score (harmonic mean of precision and recall scores) and receiver operating characteristic (ROC) analysis, which plots ROC curves and measures area under the curve (AUC), where AUC = 0.50 represents chance/random performance and 1.00 reflects perfect performance. The Cogynt model performed exceptionally well with *F1* = 0.98 and AUC = 0.99, compared with scores of 0.90 and 0.96, respectively, for the sum-of-risk model.

COMPARING APPROACHES

One might ask how the qualitative and quantitative methods compare in terms of performance. This is a complicated question, because they have been evaluated using different contexts and statistical methods. An important metric for SPJ concerns how well it lives up to the goal of increasing consistency of output, and, as noted above, it produces relatively high scores for inter-rater reliability. Metrics that focus on predictive validity (such as AUC) are more problematic for SPJ methods: AUC statistics typically range from 0.60s to mid-0.70s for SPJ tools as reported by Borum *et al.*,[44] who notes that this moderate level of performance may be the 'best that can be expected' for this predictive analytic approach. This does not compare favourably with AUC values obtained for some quantitative models, as described in the previous section. Comparison of these statistics is problematic, however, since widely differing validation methods, data and predictive criteria were used.

A more useful way to compare these modelling approaches considers their contributions to the risk assessment process (see Figure 4). Because actuarial models focus on population characteristics, application of actuarial instruments or tables may not provide the most useful approach for assessing the risk of an individual case. Qualitative SPJ models, which rely on expert judgments, provide rigorous empirically based guidelines that encourage consistency of outcomes while also benefitting from the expert's insights on a specific case. Predictive analytic models use parameters that are informed by empirical data and provide rigorous, testable predictions. AI expert system models allow domain experts to define patterns of behaviour that represent what to look for in dynamic data streams.

Computer-based methods that integrate AI expert system models with predictive analytic models provide a knowledge-driven approach that exploits the experience of

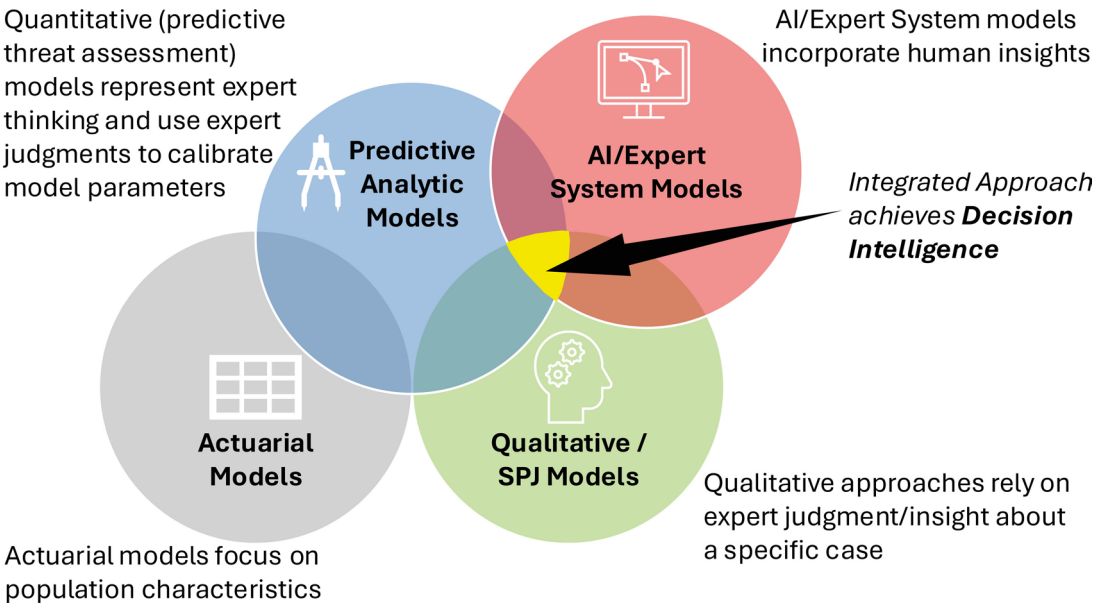

Figure 4: Comparing the contributions of different modelling approaches

experts in a transparent decision intelligence environment[45] that is distinguished from purely data-driven ML models. A more fully integrated solution that combines predictive analytics, AI expert systems and qualitative methods such as SPJ can yield a combination of methods to produce the most powerful risk management solution.

INTEGRATING QUALITATIVE AND QUANTITATIVE MODELS

Integrating qualitative and quantitative models can leverage the strengths of both methods, combining the rigour and testability of quantitative models with the insights and contextual knowledge of qualitative models. This section describes how the Cogynt model can support and enhance each step in the SPJ process.

The initial phase of the SPJ approach is to examine the evidence or input data and decide whether each of the associated risk factors is present. This triage stage is a formidable task for threat analysts, who must stay abreast of numerous events or conditions spanning months, or even years, for each individual case under consideration. A decision support tool such as the AI expert system-based Cogynt platform can track and maintain situation awareness at scale for hundreds of thousands of individuals. In the current version of Cogynt, with its built-in SOFIT PRI taxonomy, many of the indicators that have been defined and used in SPJ models are already captured in Cogynt's streaming data ingest process.

To illustrate, Figure 5 exhibits mappings from violence-risk-related SOFIT2.0 PRIs to factors used in the WAVR-21 tool (left side of figure) and the NCBIO-25 tool (right side of figure). This shows that most of the factors defined in these SPJ tools have been identified in SOFIT; it is straightforward to incorporate into SOFIT any of the SPJ factors that do not currently have direct associations with SOFIT PRIs.

Cogynt's HCEP behavioural analytic and its associated lexicon of associated key words provide automated support to identify the presence of these indicators in the available case material. This expert-informed information gathering and risk indicator accounting supports the difficult initial information processing stage of the

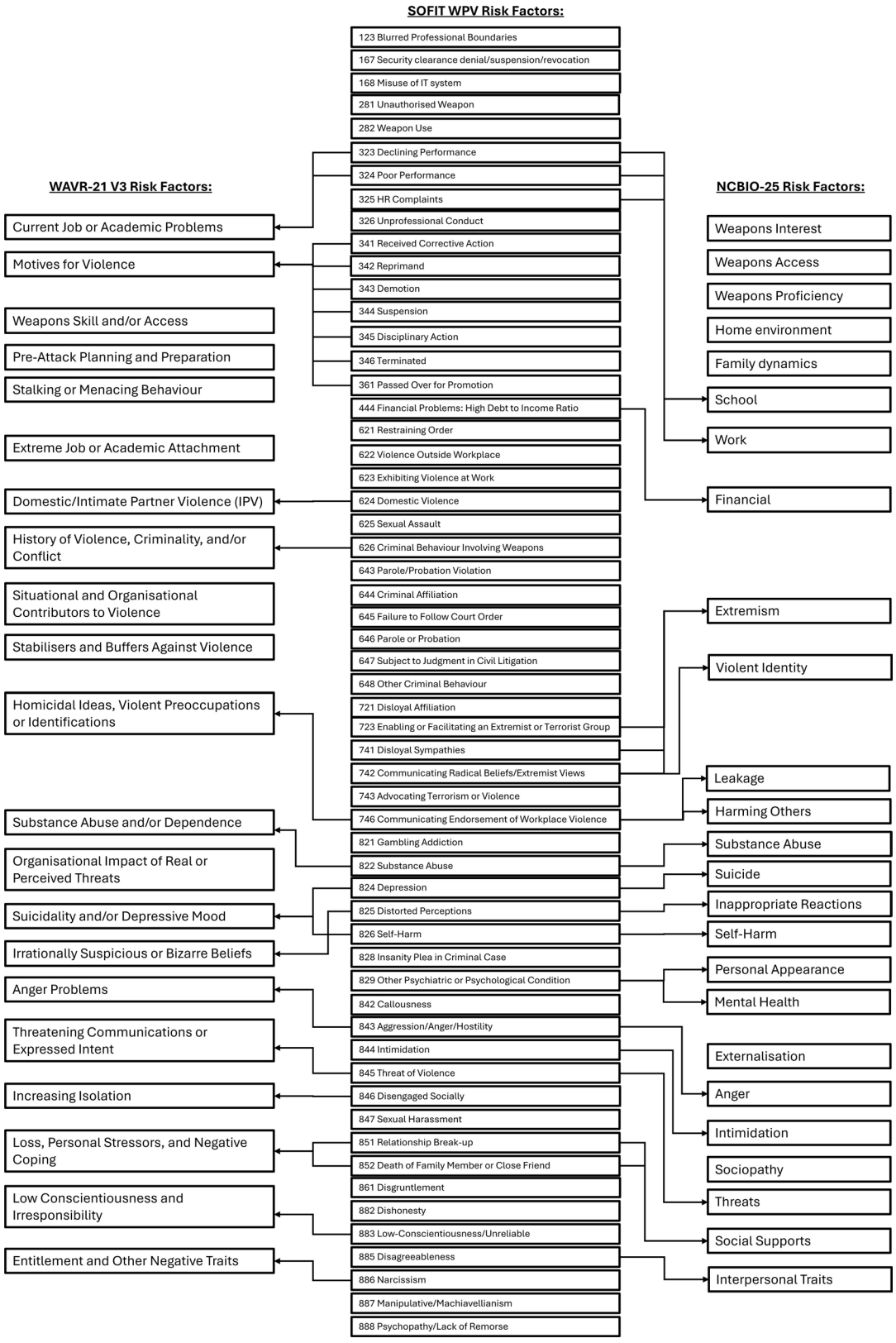

Figure 5: Mapping of SOFIT PRIs to WAVR-21 and NCBIO-25 violence risk factors

SPJ process and helps to ensure a consistent outcome.

The second step in the SPJ process is the mapping between observed risk factors and possible threat behaviours. If the SPJ approach is integrated within the Cogynt platform and applied to insider threats more generally, the identification of possible threat behaviour types is directly supported by Cogynt's HCEP model, which has been calibrated and informed by expert knowledge elicitation studies. Mappings between SOFIT PRIs and varous threat behaviours — data exfiltration/unauthorised disclosure, fraud, sabotage, espionage, workplace violence, unintentional insider threat, suicidal ideation, etc. — are included in the platform and typically adjusted as needed by users to conform with the organisation's missions and priorities.

The third step in the SPJ process, risk formulation, focuses on describing possible risk scenarios. While this stage is largely dependent on the expert analyst's judgment and insight, Cogynt's ability to summarise and tabulate observed PRIs and associated threat scenarios — coupled with its expanding, integrated AI chatbot functions — can further support this risk formulation and scenario development phase.

In the risk management and final decision/risk judgment phases, the analyst considers possible mitigation strategies, taking into account the likely scenarios and relevant protective factors, and develops final conclusions and recommendations. Importantly, risk management strategies are chosen to exploit possible protective factors that can act as stabilisers or buffers against threat behaviours. For example, a subject who is directing anger/aggression towards a coworker may be attending counselling sessions around this issue. Perhaps the subject also has a well-developed support system in friends or family members who encourage counselling sessions and good behaviour. A lack of violent history may also be considered to be a positive protective factor. All relevant protective factors are considered when formulating possible mitigation steps; in this example, mandatory counselling is an obvious recommendation as a condition for continued employment. The final judgment may also provide a risk rating that reflects the degree of severity given the observed risk factors (eg the WAVR-21 SPJ tool offers an overall risk rating of low, medium or high).

The Cogynt risk assessment model supports development and tracking of quantitative risk scores, informed initially by SOFIT PRI risk weights (but adjusted as desired based on the discretion and judgment of the threat assessment team). The threat assessment team can incorporate any desired risk calculation; Cogynt's built-in pattern-based risk propagation model has several advantages over more simplistic formulations that make unrealistic assumptions about interactions among PRIs (or lack of interactions). The Cogynt risk calculation is transparent, fully explainable and subject to the analyst's oversight. For example, the analyst can adjust the contribution of any PRI if they deem it appropriate based on unique contextual information and circumstances.

Generally, SPJ proponents eschew the use of quantitative risk scoring. Arguably, however, the SPJ use of an ordinal 'low–medium–high' rating effectively yields a quantitative outcome. For risk assessment approaches such as NCBIO-25 that wish to avoid numeric scores, the Cogynt behavioural analytic threat assessment platform can still provide a powerful decision support environment for identifying PRIs from case data, mapping PRIs to threat types, and tabulating or summarising all the appropriate evidence to support the risk assessment.

Even without the quantitative risk calculation, the system's case management functions help the analyst keep track of myriad concerning behaviours occurring over long periods of time, for a large number of individuals. For example, the drill-down

display (see Figure 6) provides a visual representation, at virtually any degree of detail, that reveals how the obtained evidence maps to each potential risk behaviour. In the example shown, the preponderance of the accumulated evidence points to a potential exfiltration incident, with relevant risk indicators relating to cyber security violations, concerning behaviours, job performance and psychosocial factors. These expert-informed relationships and patterns can readily be adapted to directly support the planning, risk management and decision stages of the SPJ process.

CONCLUSION

In conclusion, both qualitative and quantitative modelling approaches rely on human judgment. Quantitative models, such as Cogynt, represent expert thinking, with parameters informed by expert judgments tailored to the organisation's mission and priorities. Qualitative models are also informed by expert judgments. Both methods can be used to implement proactive, whole-person risk management strategies.

Rather than furthering the traditional rivalry between these approaches, however, a more enlightened path may be possible through their integration. Combining qualitative and quantitative reasoning can offer a powerful threat assessment solution. By leveraging the strengths of both methods, organisations can develop more effective risk management strategies that incorporate human judgment, data science and AI.

This paper has described how this integrated, holistic approach combines the insight and expertise of human analysts with an automated, streaming intelligence platform, using the AI expert-informed Cogynt HCEP behavioural analytic model. This produces a state-of-the-art decision intelligence solution[46] that fulfils the promise of 'joint cognitive systems'.[47] It is hoped that this proposed paradigm shift — integrating these historically divergent methods — will enhance our ability to anticipate and mitigate

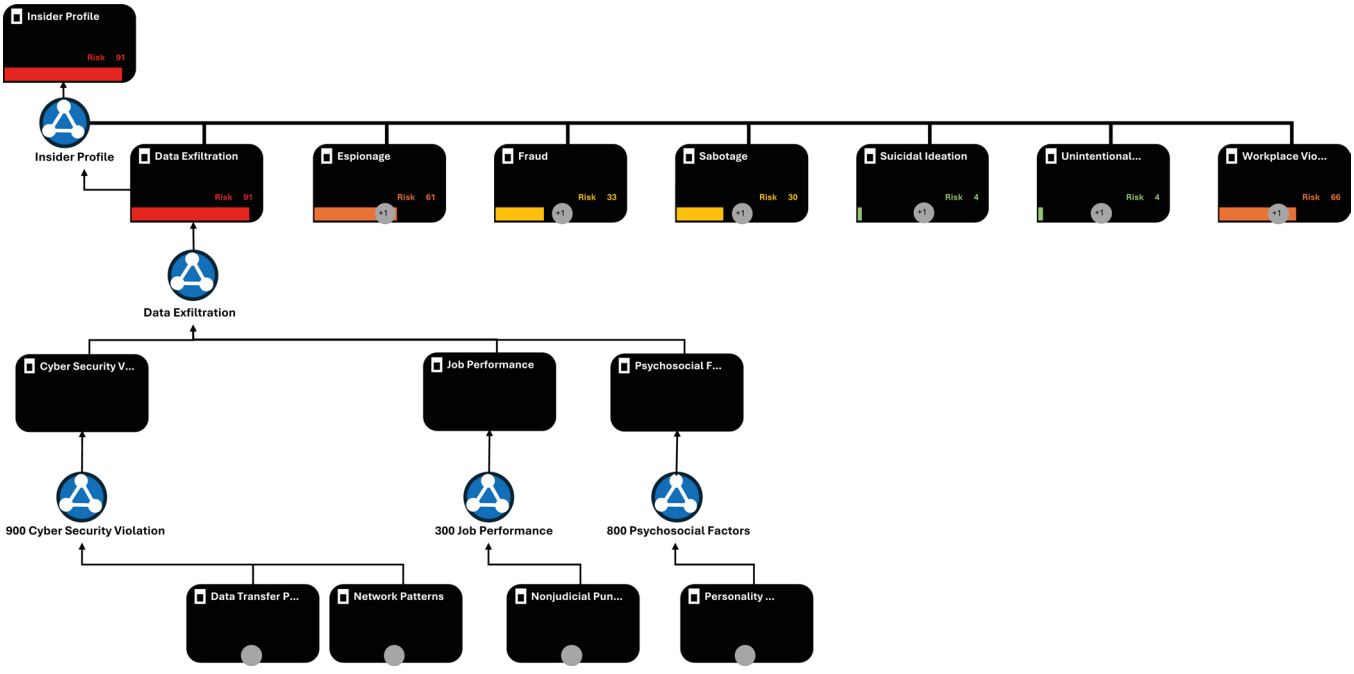

Figure 6: Cogynt drill-down display

threats with unprecedented precision and foresight.

References and Notes

1. Cappelli, D., Moore, A. and Trzeciak, R. (2012), *The CERT Guide to Insider Threats*, Addison-Wesley, Edinburgh.
2. Cybersecurity Insiders (2025), '2025 Insider Risk Report: The shift to predictive whole-person insider risk management', available at https://cogility.com/resources/insider-risk-report/ (accessed 2nd December, 2025).
3. Peterson, J. K. and Densley, J. A. (2019), 'The violence project database of mass shootings in the United States, 1966–2019', The Violence Project, available at https://www.theviolenceproject.org (accessed 2nd December, 2025).
4. Cybersecurity Insiders, ref. 2 above.
5. Department of Homeland Security (2017), 'Countering Violent Extremism: The Use of Assessment Tools for Measuring Violence Risk', available at https://www.dhs.gov/sites/default/files/publications/OPSR_TP_CVE-Use-Assessment-Tools-Measuring-Violence-Risk_Literature-Review_March2017-508.pdf#:~:text=The%20emergence%20of%20violent%20extremism%20in%20the,radicalization%20and%20divert%20individuals%20away%20from%20violence (accessed 2nd December, 2025).
6. National Counterintelligence and Security Center, 'Insider Threat Program Maturity Program', available at https://www.odni.gov/files/NCSC/documents/nittf/20240926_NITTF-Maturity-Framework.pdf (accessed 2nd December, 2025).
7. Amman, M., Bowlin, M., Buckles, L., Burton, K. C., Brunell, K. F., Gibson, K. A., Griffin, S. H., Kennedy, K. and Robins, C. J. (2017), 'Making prevention a reality: Identifying, assessing, and managing the threat of targeted attacks', US Department of Justice, Federal Bureau of Investigation (FBI), available at https://www.fbi.gov/file-repository/making-prevention-a-reality.pdf/view (accessed 2nd December, 2025).
8. Shaw, E. D. (2006), 'The role of behavioral research and profiling in malicious cyber insider investigations', *Digital Investigation*, Vol. 3, No. 1, pp. 20–31.
9. Cappelli *et al.*, ref. 1 above.
10. Greitzer, F. L. (April 2019), 'Insider Threat: It's the HUMAN, Stupid!', *Proceedings of the Northwest Cybersecurity Symposium*, No. 4, pp. 1–8.
11. Borum, R., Scalora, M., Otto, R., Schneider, K., Kennedy, K., VanBerschot, J., Mix, E. and Jaros, S. (2022), 'Structured Professional Judgment (SPJ) tools: A reference guide for Counter-Insider Threat (C-InT) hubs', Defense Personnel and Security Research Center (PERSEREC), available at https://www.cdse.edu/Portals/124/Documents/jobaids/insider/SPJ-Reference-Guide.pdf (accessed 2nd December, 2025).
12. Williams, M. M., Jones, N. T., Cilke, T. R. R., Gibson, K. A., Gray A. E. and O'Shea, C. L. (March 2024), 'Assessing the reliability and validity of the North Carolina BeTA Investigation Overview-25 (NCBIO-25) in a sample of active shooters and persons of concern', *Journal of Threat Assessment and Management*, APA OsychNet, available at https://dx.doi.org/10.1037/tam0000231 (accessed 2nd December, 2025).
13. Greitzer, F. L., Purl, J., Leong, Y. M. and Becker, D. E. (2018), 'SOFIT: Sociotechnical and Organizational Factors for Insider Threat', IEEE Symposium on Security and Privacy Workshops, pp. 197–206.
14. Amman *et al.*, ref. 7 above.
15. Greitzer *et al.*, ref. 13 above.
16. An updated version (SOFIT2.0) is available at: Greitzer, F. L., 'An Updated SOFIT2.0 Insider Threat Indicator Taxonomy', Cogility, available at https://cogility.com/blog/updated-sofit2-insider-threat-indicator-taxonomy/ (accessed 2nd December, 2025).
17. Shaw, E. D. and Sellers, L. (2015), 'Application of the critical-path method to evaluate insider risks', *Studies in Intelligence*, Vol. 59, No. 2, pp. 41–48.
18. Lenzenweger, M. F. and Shaw, E. D. (2022), 'The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions', *Counter-Insider Threat Research and Practice*, Vol. 1, No. 1.
19. SOFIT also includes an organisational factors branch (not shown) that lists organisational/environmental factors that contribute to insider risk.
20. Shaw, E. D. (2023), *The Psychology of Insider Risk: Detection, Investigation and Case Management*, Taylor & Francis Group/CRC Press, Boca Raton, FL.
21. *Ibid*.
22. Meloy, J. R., White, S. G. and Hart, S. (2013), 'Workplace Assessment of Targeted Violence Risk: The development and reliability of the WAVR-21', *Journal of Behavioral Science*, Vol. 58, No. 5, pp. 1353–1358.
23. Jones, N. T., Gray, A. E. and Williams, M. M. (2021), 'The North Carolina BeTA Investigation Overview (NCBIO-25): A structured professional judgment tool (SPJ) for behavioral threat assessment in law enforcement settings', *Journal of Threat Assessment and Management*, Vol. 8, No. 4, pp. 145–158.
24. *Ibid*.
25. *Ibid*.
26. Borum *et al.*, ref. 11 above.
27. Department of Homeland Security, ref. 5 above.
28. Borum *et al.*, ref. 11 above.
29. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M. and Gritzalis, D. (2010), 'An Insider Threat Prediction Model', in S. Katsikas, S., Lopez, J. and Soriano, M. (eds), *7th International Conference on Trust, Privacy, and Security in Digital Business: TrustBus 2010, Biblao, Spain, August 30–31, 2010, Proceedings*, Springer, Berlin, pp. 26–37.
30. Legg, P. A., Buckley, O., Goldsmith, M. and Creese, S. (2015), 'Automated insider threat detection system using user and role-based profile assessment', *IEEE Systems Journal*, Vol. 99, No. 2, pp. 1–10.

31. Legg, P. A. (2017), 'Human–Machine Decision Support Systems for Insider Threat Detection', in Palomares Carrascosa, I., Kaluratage, H. K. and Huang, Y. (eds), *Data Analytics and Decision Support for Cybersecurity*, Springer, Berlin, pp. 33–54.
32. Greitzer *et al.*, ref. 13 above.
33. Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. and Hohimer, R. E. (2012), 'Identifying at-risk employees: A behavioral model for predicting potential insider threats', Proceedings of the Hawaii International Conference on System Sciences, Maui, HI, 4th–7th January, pp. 2392–2401.
34. Axelrad, E. T., Sticha, P. J., Brdiczka, O. and Shen, J. (May 2013), 'A Bayesian network model for predicting insider threats', Proceedings of the 2013 IEEE Security and Privacy Workshops (SPW'13), San Francisco, CA, USA, pp. 82–89.
35. Elmrabit, N., Yang, S. H., Yang, L. and Zhou, H. (2020), 'Insider threat risk prediction based on Bayesian network', *Computers & Security*, Vol. 96, 101908.
36. Greitzer, F. L., Purl, J., Sticha, P. J., Yu, M. C. and Lee, J. (2021), 'Use of expert judgments to inform Bayesian models of insider threat risk', *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, Vol. 12, No. 2, pp. 3–47.
37. Greitzer *et al.*, ref. 13 above.
38. Elmrabit *et al.*, ref. 35 above.
39. Greitzer *et al.*, ref. 13 above.
40. Greitzer *et al.*, ref. 36 above.
41. Greitzer *et al.*, ref. 13 above.
42. Greitzer *et al.*, ref. 36 above.
43. Greitzer, F. L., 'From patterns to predictions: Insider risk modeling with a pattern-based behavioral analytic model', paper submitted for publication.
44. Borum *et al.*, ref. 11 above.
45. Gartner (July 2024), 'Market Guide for Decision Intelligence Platforms', available at https://www.gartner.com/en/documents/5599159 (accessed 2nd December, 2025).
46. *Ibid*.
47. Hollnagel, E. and Woods, D. D. (2005), *Joint Cognitive Systems: Foundations of Cognitive Systems Engineering*, CRC Press, New York.