CorporateLiveWire

FRAUD & WHITE COLLAR CRIME 2016

EXPERT GUIDE

www.corporatelivewire.com

withersworldwide

UNIVERSITY OF LEEDS

CREST CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

NAVIGANT

Alexander Stein, PhD
alexanderstein@dolusadvisors.com
+1 212 242 7126
www.dolusadvisors.com

DOLUS | Advisors

Human Factor Risks

By Alexander Stein, PhD, Founder, Dolus Advisors (NY)

People are the central element of fraud, cybercrime and white-collar malfeasance. Yet the ferocious complexities of human factor risks are serially underestimated.

"The biggest problem in cybersecurity," according to Linus Barloon, the Director of Cyber Security for the Sergeant at Arms of the U.S. Senate, "is a deep lack of understanding about people." In our experience, this is an accurate assessment, and also holds true within many organisations, as well as in agencies and firms engaged to provide malicious threat mitigation and defence services.

Nonetheless, businesses routinely invest considerable capital and other resources in mechanistic detect and defend prescriptions and technologies. According to a study by The Bureau of Justice Assistance produced under the aegis of the US Department of Justice, annual losses from white-collar crimes are conservatively estimated at US$426 billion to US$1.7 trillion. And The Association of Certified Fraud Examiners' "Report to the Nations" estimates that the typical organisation loses 5% of gross revenue each year to fraud. That translates to a potential projected annual global fraud loss of nearly US$3.7 trillion. The costs and losses attributable to cybercrimes are no less staggering: Lloyd's, the British insurance company, estimates that cyber-attacks cost businesses roughly US$400 billion a year, including direct damage plus post-attack disruption to normal business operations. Approximately US$77 billion are spent annually by organisations worldwide (as quantified in a report issued by the IT advisory firm Gartner) in cybersecurity technologies and services.

By contrast, expenditures ear-marked for behavioural analytics, root cause analyses, non-financial risk, and human factor risk management are disproportionately less. Attention to the mechanics of deeds frequently eclipses consideration of the actors who commit them.

Consequently, though most business leaders would agree that prevention is preferable to recovery, reactive crisis triage is the norm, and proactive pre-emption the exception. Many companies go about their business falsely assured, unaware of rakes-in-the-grass and shadow risks to which they remain vulnerable. The most critical include:

- Recognising that good solutions start with understanding the problem—human factor and soft data problems are usually misdiagnosed, oversimplified, or defined in superficial language;
- Why good people sometimes do bad things—understanding the drivers of malicious decision-making and behaviour;
- Fraud, ethics, and compliance problems aren't avoided or resolved with good plans—there is a broad delta between blueprint and reality regarding ideal conduct and actual human propensities.

These and other blind-spots inevitably derogate countless structures and functions intended to monitor, regulate, mitigate, control, or remediate various risks. Many other countermeasures are compromised by the resultant compounding technical and conceptual debts. And these, in turn, give rise to clusters of waterfall issues with which compliance, risk, info-sec officers, and other business line directors are at a loss to address. We repeatedly encounter organisations struggling against knowledge and expertise gaps in understanding or addressing integral human factor issues.

Among the most prevalent and damaging are misnomers regarding the presumptive causal links between motivation and behaviour, and the assumed line between behavioural signals—so-called 'red flags'—and imminent lawless action. These are mistakenly understood as binary cause-and-effect systems. That yields an established but incorrect solutions-oriented formulation: determining why somebody does bad things—bites the hand that feeds him, takes what belongs to others, behaves unethically or immorally, goes rogue—will inform a standardised actionable means of prevention. While plausible in theory, it adds little to developing useful counter-measures.

“Conventional approaches to threat detection hinge on monitoring and deriving conclusions from what people literally say or write.”

De-coupling motivation from behaviour helps to revise this misconception. While some actions may be traceable to an obvious originating impulse, many are not; there is no direct drive train between thought and action. In mental functioning, it does not hold universally true that ‘X’ happened because of ‘Y’. One source of confusion stems from criminal law: legal theory and doctrine regarding the guilty mind, guilty act, and knowledge of illegality and intent to harm are requisites to a court’s determining penalty. But these judicial concepts are largely agnostic to the actual underlying generators of malfeasance; the jurisprudential definitions and psychological explanations of intent are not synonymous. The idea that a clearly identified motivation factor will yield a predictable behavioural outcome is a base fallacy which unavoidably degrades otherwise well-designed defence and detection protocols.

Lying, deception, opacity, manipulativeness, duplicitousness, evasiveness, secretiveness, and self-interest are all closely associated with criminal deviance and malfeasance. But they are also normal, garden-variety psychological devices. People employ contrivance and deception as coping devices and for self-preservation in a million circumstances, ranging from the innocuous, daily social falsities that are mainstays of communal life to the avoidance, obfuscation, or concealment of anxieties, embarrassments, inadequacies, or key aspects of self. Everyone hides or disguises a nearly infinite range of thoughts, feelings, impulses, or desires in order to avoid scrutiny, punishment, humiliation, or to preserve emotional homeostasis. There need be no other person or even any actual external threat. We are all masters of self-generated self-deception, magical thinking, and fantastical delusion. As André Malraux, the early 20th Century French novelist and art historian, observed, “Man is not what he thinks he is; he is what he hides.”

People who know each other very well successfully deceive one other about all manner of things every day. Walk into any organisation—even those with a cultivated culture of ethics and compliance, where leaders and boards collaborate, regulatory mandates align with institutional practices, employees and managers are respectful and collegial, people are compensated fairly, and regulations and expectations for conduct, performance, and advancement are sensible—and there will still always be a dizzyingly complex collection of individuals interacting in densely layered relationships. Roles, titles, and professional behaviour notwithstanding, everyone navigates his or her unique experience of the world in ways largely invisible and unknown to anyone else.

Communication is of course central to our existence as individuals and as social animals. And so decoding spoken and written communication data, which hold the potential to signal many risks or impending threats, are critical facets of mitigating malfeasance. But understanding those signals, typically more semaphore than billboard, is complicated. People frequently say things they don’t necessarily mean. They also don’t always know themselves what they mean or how they’re being received by others, and very often reveal more (or less, or something else) than they realise or intend.

Conventional approaches to threat detection hinge on monitoring and deriving conclusions from what people literally say or write. Invariably missed are the shadow narratives—what people imply, don’t say, seem to say, or hint at by non-verbal gestures and cues. The complexities of these nuanced elements are intensified in scenarios where dissembling, distortion, and distraction are intentional (whether or not malice is afoot), or in nefarious schemes involving stealth, guile, seduction, or inducement.

Taken together, the foregoing helps to explain the hallmark reaction of surprise on learning that a seemingly ‘good person’ has ‘gone bad’, and why hindsight is proportionally keener than foresight. It also sheds light on understanding why it’s not only unequivocally bad actors who can wreak havoc. Many otherwise responsible executives and corporate citizens precipitously become negligent or unwitting insiders for reasons unconnected to malice, thievery, or misanthropy. Some may be wilfully destructive, but the wreckage they create is an unintended by-product rather than a goal. Yet others may be irresponsible, anxious, insecure, or immature; their actions could be attributable more to paralysing fear and execrable judgment than Machiavellian indifference. Though “slippery slopes,” “rotten apples,” “rogues,” and “lone wolves” remain popular descriptors, there are many interlacing ingredients and potential triggers leading to malicious acts. Conventional thinking notwithstanding, early warning signs of impending events are inordinately difficult to discern and accurately interpret.

On the basis of such inaccuracies, organisations go to great lengths to identify and deter crooked needles. While not without value, these initiatives infrequently, or inadequately, address the matrix of underlying soft factors in the haystack that incrementally incubate malicious attacks and facilitate malicious actors.

Forecasting human risk is very different from predicting financial market undulations, weather systems, athletic performance, social and economic trends, migration patterns, or election outcomes. It involves specialised expertise in soft data and human factor analysis

“There are no simple solutions for such complex issues. But there are several perspective shifts business leaders and compliance and security professionals can adopt to re-frame and enhance malicious insider policies and practices”

with which to cull static from noise and to triangulate actionable intelligence from fragmentary, nonsensical, inscrutable, and down-the-rabbit-hole datasets.

There are no simple solutions for such complex issues. But there are several perspective shifts business leaders and compliance and security professionals can adopt to re-frame and enhance malicious insider policies and practices:

- *Malfeasance will only rarely be prevented or deterred by legislation, regulation, or data analytics alone.* Revamped threat intelligence protocols, regulatory statutes, ethics, compliance, and conduct codes are insufficient, no matter how rigorously architected. In fact, these initiatives often amplify, rather than reduce, risk. How? Conventional programs seek to channel behaviour toward an ideal or to establish deterrents. Consequently, workers are pincered between an aspiration or a punishment. While people can be discouraged, restrained, or redirected against wrong-doing, impulses cannot be legislated. Genuinely robust malicious insider defence will account for, not contravene, the attainable realities of human propensities.

- *Model human risk similarly to transactional risk—sensibly consider probabilities not fantasies.* As already indicated, lying, deceptiveness, deviousness, manipulativeness, exploitativeness, and self-interest are universal, not exceptional or necessarily pathological, even among the most honest, trustworthy, and ethical. Policies and protocols that have no built-in impact absorption for these and other such unavoidable human traits are inviting disaster. Accordingly, institutions should avoid trying to militantly inoculate against malicious behaviour; policies, systems, and conduct codes which privilege impossible or improbable human factor scenarios are close to valueless.

- *Companies will be continually blind-sided so long as they think that merely talking about blind spots constitutes the actual address of them.* Avoid over-valuing buzz words and remain alert to the intellectual anemia they mask. Disgruntlement, greed, confirmation bias, risk aversion, and many others, are now mainstream jargon. While legitimate ideas appropriated from social science and other branches of research, they’ve become pop-psychology place-holders, diluted to near-uselessness. They do not by themselves meaningfully explain multifaceted precursor dynamics or, more importantly, provide practical applicability to detecting or mitigating malicious behaviour in real world scenarios.

- *Technology does not comprehensively address human factor risks.* Machine learning, artificial intelligence, neural networks, and other big-data platforms present potential gap-leaping advances in predictive analytics, threat intelligence analysis, and incident response. But there are substantial challenges, not all attributable to computational limitations. The primary factor pivots on the questionable foundational assumption that mental architecture and human subjectivity are quantifiably reducible to algorithmic formulation. Human behaviour and its drivers, whether veering toward nefariousness or otherwise, defy absolute correlation to more measurable data sets. Coding for decision-making in, for example, complex strategy games, autonomous vehicle control, or pattern-based problem-solving and tactical reasoning is different from predictive data interpretation regarding human intentionality. In addition, the project of resolving the thoroughly self-inflicted human problem of malfeasance by technological means, attenuates core misunderstandings about the nature of the problem itself.

Robust organisational security—whether against fraud, corruption, bribery, money laundering, cybercrime, or a multitude of other malfeasance risks—is a multidisciplinary enterprise. Effective detection, defense, mitigation, and redress programs need to synergistically harmonise the skills and interests of all institutional stakeholders. And must also involve specialists in the central, critical factor: the human mind.

Dolus Advisors is a boutique New York-based consultancy that employs expertise in human risk forecasting and the psychodynamics of fraud, corporate ethics, compliance, and organizational culture to help companies proactively mitigate white-collar and cyber malfeasance risks. Founder and Managing Principal Alexander Stein is regarded as a leading authority in the psychology of fraud, and is a frequent keynote speaker and widely published writer, notably including “Warfare of the Mind: Innovations and Strategic Applications in the Psychology of Fraud” in the FraudNet World Compendium of Asset Tracing and Recovery (2nd Ed).