EUROPEAN JOURNAL OF INFORMATION SYSTEMS
https://doi.org/10.1080/0960085X.2022.2088414

THE OPERATIONAL RESEARCH SOCIETY
Taylor & Francis
Taylor & Francis Group

EMPIRICAL RESEARCH

Adopting and integrating cyber-threat intelligence in a commercial organization

James Kotsias[a], Atif Ahmad[b] and Rens Scheepers[c]

[a]Advantage Cyber, Melbourne, Victoria, Australia; [b]School of Computing & Information Systems, Faculty of Engineering and IT, University of Melbourne, Parkville, Victoria, Australia; [c]Department of Information Systems and Business Analytics, Deakin Business School, Deakin University, 221 Burwood Highway, Burwood, VIC 3125, Australia

ABSTRACT

Cyber-attacks are increasingly perpetrated by organised, sophisticated and persistent entities such as crime syndicates and paramilitary forces. Even commercial firms that fully comply with industry "best practice" cyber security standards cannot cope with military-style cyber-attacks. We posit that the primary reason is the increasing asymmetry between the cyber-offensive capability of attackers and the cyber-defensive capability of commercial organisations. A key avenue to resolve this asymmetry is for organisations to leverage cyber-threat intelligence (CTI) to direct their cyber-defence. How can commercial organisations adopt and integrate CTI to routinely defend their information systems and resources from increasingly advanced cyber-attacks? There is limited know-how on how to package CTI to inform the practices of enterprise-wide stakeholders. This clinical research describes a practitioner-researcher's experiences in directing a large multinational finance corporation to adopt and integrate CTI to transform cybersecurity-related practice and behaviour[1]. The research contributes practical know-how on the organisational adoption and integration of CTI, enacted through the transformation of cybersecurity practice, and enterprise-wide implementation of a novel solution to package CTI for commercial contexts. The study illustrates the inputs, processes, and outputs in clinical research as a genre of action research.

ARTICLE HISTORY
Received 14 September 2020
Accepted 7 June 2022

KEYWORDS
Cybersecurity; information security management; cyber defence; incident response; threat intelligence; clinical information systems practice

1. Introduction

Cybersecurity is a critical concern for organisations globally.[1] Cyber-attackers target organisational information and systems resources for financial gain or geo-political imperatives. This includes theft of sensitive customer data, intellectual property, confidential plans relating to business strategy, and disruption of mission-critical IT systems. The cyber-threat landscape has shifted in recent years with the emergence of organised crime syndicates and nation-state paramilitary cyber entities. Terminology such as advanced persistent threats (APTs) are now used to describe such entities (Ahmad et al., 2019; Lemay et al., 2018). APTs are increasingly sophisticated, recruiting IT experts into purpose-built teams and deploying military-grade cyber weaponry in high-precision attacks against selected targets.

In contrast, organisational cyber-defences have not evolved at the same rate. Many commercial organisations have institutionalised complex cybersecurity structures to comply with obligations imposed by law, regulation, general "best practice" industry frameworks and standards. Consequently, organisations find themselves in an asymmetrical arms-race against cyber-threat actors that are so agile and aggressive that they can bypass or overwhelm even the most sophisticated cyber defences. High-value organisations have to defend against a massive volume of cyber-attacks on a daily basis. The same principles that have established organisations' asymmetry vis-a-vis cyber attackers may also hold the answer to resolving it. This would imply that commercial organisations adopt military-inspired principles to defend themselves, given the nature of the emerging cyber threat landscape.

Military organisations have long understood the invaluable role that threat intelligence plays in directing operations against hostile actors. In similar vein, we argue that cyber-threat intelligence has a critical role to play in redressing the asymmetrical advantage to cyber-attackers over cyber-defenders. Cyber threat intelligence (CTI) is the process of "acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities inside the cyber domain to offer courses of action that enhance decision making" (Ettinger, 2019). CTI thus has the potential to change organisations' cybersecurity behaviour from being reactive to "proactive, anticipatory and dynamic" (Shin & Lowry, 2020, p. 6). CTI can play a critical role in directing organisational behaviour in prevention, detection and response to cyber-attacks. For example, CTI can

CONTACT Atif Ahmad atif@unimelb.edu.au School of Computing & Information Systems, Faculty of Engineering and IT, University of Melbourne, Parkville, Victoria, Australia

support prevention by alerting organisations to vulnerabilities that can exploited by specific threat actors with the means, motivation and capability to attack the firm. CTI can assist in detection of cyber-attacks by tasking intrusion detection systems to patterns of exploitation related to specific threat actors. And, CTI can direct cyber-response by providing a precise defence strategy to combat a cyber-threat actor's modus operandi (Shin & Lowry, 2020 p. 1; Ettinger, 2019). Therefore, organisations' ability to assimilate and operationalise cyber threat intelligence on a routine basis is central in this regard.

For commercial organisations, the adoption of CTI poses several challenges. The military mindset associated with the use of threat intelligence is foreign to the typical business culture that prevails in many of these organisations. Given the emerging cyber-militarised threat environment, there is limited know-how about the deployment and routinisation of CTI to inform actions of executives and business managers. Moreover, many of these organisations would need to transform their cybersecurity practice from a predominantly compliance-driven and reactive logic towards a proactive logic driven by CTI.

How can commercial organisations adopt and integrate cyber threat intelligence to transform their cyber defence behaviour from being reactive and undirected to being proactive and directed? The paper describes how a practitioner-researcher addressed this clinical problem in a large multinational corporation that transformed their cybersecurity practice towards a CTI-driven approach. The practitioner-researcher is the corporation's Global Cyber Strategy Lead. The clinical research reported in this paper draws on the practitioner-researcher's practical experience in cybersecurity management and on his research expertise developed in partnership with researcher-practitioners (in this case Information Systems and Cybersecurity scholars; cf., Iversen et al., 2004; Schön, 1983).

The paper is structured as follows. To situate the clinical research, we review literature pertinent to the emerging cybersecurity threat landscape and the use of CTI in organisations. We then describe the research approach followed by the practitioner-researcher in two phases. In phase 1, the case organisation adopted CTI as innovation in its IT Operations Division. In phase 2 the innovation is translated into a novel solution – CTI-as-a-service – as a means to package and integrate CTI into the broader commercial context and for business users. We describe the enterprise-wide integration of CTI-as-a-service, including concomitant interventions to influence managerial behaviour and risk calculus. We reflect on the adoption and integration of CTI, evaluating how the organisation has adapted its cybersecurity posture to better cope with the evolving cyber-militarised threat landscape.

2. Literature review

The increasing complexity of technology infrastructures, hyperconnectivity in the modern era, and the targeted use of military-grade cyber weaponry poses a significant and escalating risk to private enterprise (Baskerville et al., 2014; Shin & Lowry, 2020). Recent industry reports highlight the increasing disparity between the capability of "Advanced Persistent Threats" (APTs) to penetrate organisations and the capability of commercial organisations to defend themselves (Microsoft Corporation, 2020; Verizon Corporation, 2018). An Advanced Persistent Threat is defined as an "entity that engages in a malicious, organized, and highly sophisticated long-term or reiterated network intrusion and exploitation operation to obtain information from a target organization, sabotage its operations, or both" (Ahmad et al., 2019, p. 406).

The underlying reason for this disparity is that the increasing sophistication and militarisation of the cyber threat landscape has not been met by a commensurate re-orientation of cyber defence in private enterprise (Shin & Lowry, 2020). APTs invest their time and resources studying the cyber defences of their targets and experimenting with novel ways to penetrate and acquire their mission objectives (e.g., theft of IP and/or disruption of IT services; Ahmad et al., 2019). In contrast, private enterprise has long adopted an inward perspective aimed at complying with general industry cybersecurity standards while remaining largely oblivious to the activities of cyber-threat actors. Consequently, while many commercial organisations invest in high levels of general cyber-readiness, they lack sufficient *situation awareness* of the threat landscape and adversaries to develop the required defensive capabilities (Ahmad et al., 2021).

As Baskerville (2005) pointed out almost two decades ago, the prevailing prevention paradigm assumes risks can be anticipated, measured, and quantifiably mitigated in advance using cybersecurity controls. This paradigm renders risk management a problem of compliance, rooted in the probabilities of known attacks. Instead, Baskerville (2005) advocates for possibilistic thinking in cyber defence. Indeed, this mode of thinking is applicable, given developments in the cybersecurity threat landscape in recent times. In particular, the possibilistic paradigm seems more appropriate in the light of novel and innovative means of attack. Such cyber-attacks are dynamic and their risks cannot be quantified in advance. Thus, organisations have to turn to threat intelligence as a means of responding to highly unpredictable and insidious cyber threats. This is in line with Sun Tzu's famous metaphor in his Art of War (Giles, 1910): *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not*

the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle".

Shin and Lowry (2020) interpret Sun Tzu's advice to "know the enemy" as a call for CTI that ultimately requires organisations to shift their culture of risk management from compliance with general industry standards towards threat intelligence collection and operationalisation. They further explain the fine distinction between general readiness and readiness to defend against specific adversaries as follows: " ... *imagine that a boxer trains to improve his/her defenses in advance of a match. First, the boxer can try to improve his/her general defense skills without regard to the upcoming opponent. Second, the boxer can also train in a manner tailored to the opponent's offensive style. A boxer can thus increase his/her odds of success by mastering both general defense and defense tailored to an opponent's unique offensive strengths*" (p. 3).

A more detailed definition of CTI is " ... contextualized output of a strategically-driven process of collection and analysis of information pertaining to the identities, goals, motivations, tools and tactics of malicious entities intending to harm or undermine a targeted organization's operations, ICT systems or the information flowing through them" (Bank of England, 2016, p. 12). CTI thus encompasses evidence-based knowledge that can include context, mechanisms, indicators, implications and/or advice (Holland, 2015; Samtani et al., 2020; Schlette et al., 2021). In most cases CTI is aimed at cybersecurity professionals as it enables them to proactively defend against attack, reactively detect and diagnose a breach and prioritise incidents based on risk exposure.

CTI enables cybersecurity professionals to develop situation awareness of the incident environment and the "attack surface" (the sum of all vectors of attack to penetrate an organisation; Shin & Lowry, 2020). CTI is also a key enabler for cyber defence, for example, tracking and breaking the attacker's kill-chain (reconnaissance, weaponisation, delivery, exploitation, installation, command & control, actions on objective; Hutchins et al., 2011). However, CTI is also critical for general managerial and executive stakeholders as it helps them to understand their risk exposure and the options they have to mitigate potential impacts.

In organisational contexts, CTI functions have the responsibility to identify an organisation's intelligence requirements, collect relevant information from a range of internal and external sources and develop insights that can be used to inform action and decision-making. This involves synthesising external and organisation-specific sources to produce tailored intelligence that can be disseminated to specific internal users (Lawson et al., 2019; Webb et al., 2014). Numerous vendors (e.g., Crowdstrike, FireEye/Mandiant, Kaspersky, Anomali, RecordedFuture) have responded to the increasing demand for CTI by providing services that promise stronger cyber defences, reduced incident response time, and improved strategic decision-making (Crowdstrike, 2021).

The utility of CTI to decision-makers is contingent on the quality of CTI. Quality of CTI can be measured against nine criteria, mirroring the quality indicators of the US Army's keystone manual for military intelligence (FM 2–0, 2010, pp. 1–17): (1) *Accurate* (presents objective reality), (2) *Relevant* (supports the decision-makers conceptualisation of the problem) (3) *Complete* (contains essential components required for decision-making), (4) *Precise* (provides the level of detail and complexity required for decision-making), (5) *Timely* (is presented as early as possible for decision-making), (6) *Usable* (is easily understood and meaningful to the decision-maker), (7) *Reliable* (presents trustworthy content), (8) *Predictive* (anticipates future events significant to decision-maker) and (9) *Tailored* (supports and satisfies decision-maker priorities).

Despite the existence and utility of vendor-supplied CTI services and general industry guidelines on best practice in cybersecurity, there is very little practical guidance in the literature on how organisations can adopt and integrate CTI. The literature on CTI adoption focuses on the technical aspects of CTI such as event aggregation and correlation, machine-based AI techniques for real-time threat hunting as well as post-incident forensic analysis of malware and intrusions (Samtani et al., 2020). It remains unclear how CTI can be incorporated into routine organisational practices to direct cybersecurity defence against APTs. More broadly, the literature is largely silent on how commercial organisations' culture and processes can be re-oriented to a level of military-style "readiness" to address sophisticated cyber-attacks.

3. Clinical case: adopting and integrating CTI at greenback financial

Greenback Financial (pseudonym) is a large multinational finance corporation with a market capitalisation of over fifty billion US dollars, operating in 34 countries spanning North and South America, Central and Southern Asia, Europe, and Oceania. The corporation employs sixty thousand personnel world-wide. From a cybersecurity perspective, the firm's primary strategic-level objectives are (1) to maintain the continuity of its global digital platforms and services and (2) to protect the confidentiality of sensitive organisational and customer data. Greenback Financial experiences almost twenty billion cybersecurity-related data events every 24 hours. These events are generated from across the firm's diverse global technology infrastructure. To protect the firm from cyber-attacks the firm's

IT Operations division features a dedicated 25-person strong Security Operations Centre (SOC) that monitors and responds to cybersecurity attacks.

3.1. Clinical research processes and framework

The clinical research process followed in this study is action research (Avison et al., 1999; Baskerville & Wood-Harper,1998; Iversen et al., 2004). As advocated in the action research methodology literature, this includes initial problem realisation/reconnaissance/fact-finding phases leading to planning problem-solving activity, implementation and evaluation, with non-linear iteration cycles between the phases (McKay & Marshall, 2001). Some action research sources portray a researcher(s) interacting with practitioner(s) in a particular research setting (Baskerville & Wood-Harper, 1998). In this clinical research, the practitioner-researcher is the same individual (Schein, 1987). The research-practitioner in this study has a lived experience of the clinical situation in the organisation and is bringing education obtained through scholarly research training to bear on the research problem.

The clinical research process occurred within a broader framework of the adoption and implementation of innovations in organisations (e.g., Cooper & Zmud, 1990; Rogers, 1995; Tornatzky & Klein, 1982). In the initial adoption phase (Phase 1), the innovation (here CTI) was adopted within the IT operations division. This was followed by a subsequent integration phase (Phase 2) whereby the innovation was adapted (in the form of CTI-as-a-service) and implemented across the enterprise.

While we present the clinical action research sequentially, there were non-linear elements to the processes. For example, initial problem realisation was followed by fact-finding and planning for problem-solving. However, during these steps the practitioner would discover more about the nature and magnitude of the unfolding problem, thus requiring a return to the problem realisation step (as also noted in other action research, e.g., Iversen et al., 2004; McKay & Marshall, 2001). Similar iterations occurred during the second phase. The sections that follow describe the two phases, and actions of the research-practitioner in each phase.

This study provides a perspective on clinical research as a genre of action research. As depicted in Figure 1, the clinical research processes in this study were underpinned by four key inputs. First, the practitioner-researcher not only understands, but is deeply immersed in the clinical context (as an insider, not as outsider). Second, the practitioner draws on extensive lived personal experience (several years responsible for cyber defence strategy, and being on the frontline response to numerous cyber-attacks). Third, the practitioner draws on professional and industry practice (professional networks in the banking sector and information security industry). Fourth, the research is framed by practitioner-researcher's theoretical knowledge (of information security, adoption and implementation of innovations in organisations, socio-technical change, and research methodology). Wearing the hats of practitioner and researcher at the same time and leveraging both practical and theoretical perspectives on the research problem was instrumental to progress. Combined, these inputs informed the clinical action research processes: problem realisation & exploration, solution development & implementation, and reflection & evaluation. In turn, the inputs map onto the key outputs of the clinical research processes: CTI-as-service as the clinical solution (Table 1) and its impact on the organisation (refer Appendix), new personal experience gained by the practitioner, contribution to professional industry practice (as articulated in this publication), and a contribution to theory (refer Discussion).

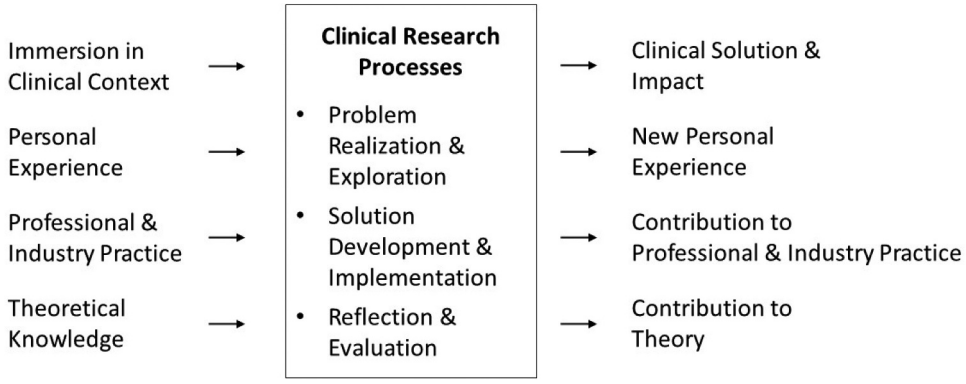

Figure 1. Clinical research processes and framework in this study.

3.2. Phase 1: CTI Adoption in the IT operations division

3.2.1. Problem realisation

Greenback Financial's market positioning, iconic status in their base region, management of large funds transfers, and status as a national-level critical infrastructure organisation makes it a high-value target for APTs. Nation-state backed APTs are interested in disrupting national commerce and reducing trust in national financial systems. As a result of being in the cross-hairs of numerous cyber threat actors, the volume, sophistication, and level of aggression of cyber-attacks experienced by Greenback has dramatically increased year-to-year.

Reflecting on the emerging cyber threat landscape, the practitioner-researcher came to the following critical realisations. First, in the absence of appropriate interventions, the unprecedented and escalating volume and sophistication of cyber-attacks will eventually overcome Greenback Financial's defences. Second, militarisation of the cyber threat landscape has created a new adversarial reality that has rendered obsolete the traditional model of compliance to conventional industry security standards. Hence a new model of cyber defence was needed: military-style cyber-attacks demand a military-style response. The ability to adopt CTI in routine operations was instrumental in this regard. Third, commercial institutions such as Greenback are not accustomed to operating with this military mindset. Greenback's managers are more focused on their customers, financial competitors and regulators rather than cyber-adversaries. Hence, the adoption of CTI as part of a new model of cyber defence would require concomitant interventions to integrate and routinise CTI into the broader organisational culture, changed managerial behaviours and enterprise-wide processes to respond to this new adversarial reality (Bostrom et al., 2009; Mumford, 2006).

3.2.2. Problem exploration

To prevent cybersecurity attacks from impacting the firm, Greenback Financial has a sophisticated multi-layered system of defences consisting of best-of-breed firewalls, intrusion detection systems, and anti-virus software augmented with specialised tools from market leading vendors (e.g., FireEye, Microsoft, Symantec). Greenback invests considerable resources into testing and refining the cyber defensive layers with bespoke code to ensure effectiveness against a broad spectrum of cyber-attacks.

For cyber monitoring and response, Greenback Financial retains a 24 × 7 security operations centre (SOC) that detects, diagnoses and investigates cyber-attacks and coordinates responses with technology operations teams (refer Figure 1). Greenback's SOC consists of three levels of security analysts that work around the clock in shifts. Level 1 analysts triage incidents, collect raw data from individual IT systems to build context which they record in a ticket management system, analyse the incident to assess criticality, and either coordinate responses or escalate to more experienced analysts depending on the criticality of the incident. Level 2 analysts are more experienced personnel that assist with load management and provide more expert advice (e.g., on false positives). Level 3 analysts acquire situation awareness of global IT operations through the use of specialised analytics tools and engage in diagnosis, investigation and coordination of high criticality incidents that may involve coordinating a large-scale response with technology operations teams.

The practitioner-researcher observed that although the SOC was expertly detecting, diagnosing and coordinating the management of incidents, the firm's response to cyber incidents was reactive, inward-looking and short sighted (i.e., Greenback Financial was unable to identify risks in the immediate future by extrapolating from previous cyber-related events). Further, the firm's cybersecurity response to attacks was insular in the sense that it was not building on knowledge and insights from other firms that had experienced similar attacks. Cybersecurity operations was able to explain "what" incidents were taking place on the IT infrastructure or "how" cyber-attacks had occurred, but was less able to answer strategic-level questions such as "why" they might be occurring or "who" might be attacking the firm and "when" they might attack next.

The practitioner-researcher concluded that Greenback Financial must respond proactively to cyber-attacks from sophisticated threat actors and adapt its prevention and response capability to the demands of an evolving threat landscape. In order to do this, a CTI function must be created and fully incorporated with existing cybersecurity operations.

3.2.3. CTI as innovation within the IT operations division

Greenback Financial retains a vast heterogenous technology estate spanning thirty-four countries situated in North and South America, Central and Southern Asia, Europe, and Oceania. To prevent and respond to cyber-attacks against the infrastructure, the firm's SOC relies very heavily on system activity logs generated by the firm's IT networks and devices. As the number of cyber-related log entries generated every 24 hours reaches approximately 20 billion, the firm uses a security incident and event management (SIEM) system to store, cross-correlate and analyse log entries to identify meaningful attack patterns. A separate custom platform (Advanced Cyber Analytics) collects behavioural monitoring data related to the activities of the firm's sixty thousand staff.

As depicted in Figure 2, the system activity logs are correlated and aggregated (arrows 1 and 2) before security alerts are generated by real-time algorithms (arrows 3 and 4). Level 1 analysts triage security alerts and determine priority after which high priority incidents are escalated (arrow 5 or 6) while low priority incidents are contained, eradicated and resolved. High severity incidents trigger the formation of a Security Leadership Team (Security LT) (arrow 7) that assesses the situation, opens communication channels to relevant stakeholders up the chain of command (arrow 11) and across the breadth of the enterprise (arrow 12). The Security LT coordinates the broad enterprise response with the support of technology and business teams.

To adopt CTI the firm created a centralised team of 4–6 specially-trained personnel that collects multi-source intelligence from national and international security and law enforcement agencies, threat intelligence vendors such as FireEye, and a closed community of intelligence specialists within the financial sector. The team monitors the threat landscape, collects and analyzes threat intelligence from the above-mentioned sources and applies adversarial thinking and frameworks (e.g., the "kill-chain" process of cyber-attacks). This enables the team to provide accurate, timely and targeted advice in the form of actionable and organisation-specific insights to security analysts in the SOC as well as the enterprise cybersecurity leadership team. Further, the firm's SOC procured specialised tools with embedded threat intelligence (e.g., indicators of compromise) to map threat patterns and prioritise which detection and responses require the most attention.

The threat intelligence team provides operational, tactical and strategic level threat intelligence through reliable and routine feeds (e.g., general alerts, bulletins) to relevant stakeholders. At an operational level, the team proactively monitors the threat landscape feeding actionable intelligence to SOC analysts (e.g., blocking IP addresses, interpreting security alerts, suggesting possible avenues of investigation) (arrow 8). At a tactical level the team predicts threat activity and validates that against the observations of the Level 3 SOC analysts (arrow 9). At a strategic-level, the team identifies new threat actors and their tactics, techniques and procedures (TTPs) to identify and address gaps in the firm's cyber defences that might be exposed (arrow 10).

Outside of the cybersecurity function, CTI was deemed to be critical to a range of executive, managerial and operational stakeholders in the broader enterprise. Therefore, CTI was supplied to these stakeholders to ensure relevant feeds, advisories and bulletins produced by CTI analysts, penetration testers, incident responders as well as specialised CTI software was distributed for decision-support purposes.

The practitioner-researcher observed that CTI adoption within IT Operations had significantly improved the cybersecurity posture by: (1) improving alignment between the activities of cyber-defence and cyber-attack, (2) reducing the success rate (and therefore impact) of cyber-attacks as the firm halts attack operations earlier rather than later, and (3) improving efficiency and focus of cyber defence operations against cyber-attacks (Refer Appendix, Table A1).

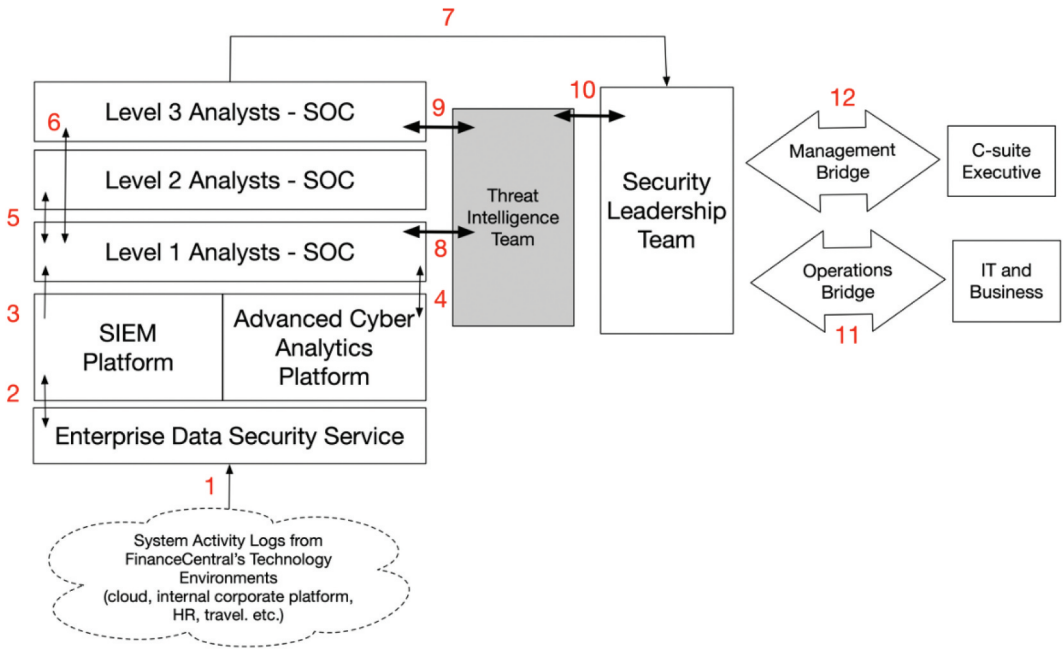

Figure 2. Adoption of CTI in the cybersecurity function of greenback financial.

3.3. Phase 2: enterprise-wide CTI integration

3.3.1. Problem realisation

Although CTI was successfully adopted, the practitioner-researcher realised that the transformation of cyber security practice was largely localised in the IT Operations unit. The cybersecurity behaviour of stakeholders across the rest of enterprise, particularly business unit managers, remained largely unaffected.

For instance, given that IT systems tend to have or develop vulnerabilities, business owners are expected to "patch" systems with the latest vendor-issued security updates. A culture of compliance holds that the higher the percentage of patches applied to vulnerable systems, the more compliant the systems are. In this context, compliance is considered to be synonymous with the level of cybersecurity. The practitioner-researcher observed a risk calculus is undertaken by asset owners in balancing the competing priorities to maintain high levels of asset uptime on the one hand and vulnerability management on the other. Vulnerability management requires systems to be taken down to apply patches which reduces uptime. Asset owners are under no obligation to resolve a vulnerability or act on threat intelligence, but instead are only expected to *consider* thresholds of acceptable risk. The practitioner-researcher observed the tendency of asset owners to simply accept the cybersecurity risk rather than allow the asset to be taken down for patching purposes. As a result, the number of fully patched systems across Greenback Financial fell to less than 40% (i.e., a randomly directed attack at an IT asset was more likely than not to hit a non-compliant system).

The practitioner-researcher also noted that when provided with specific threat intelligence of attack, some owners were more likely to instal patches on vulnerable IT systems. Although this was promising, large-scale acceptance of CTI across global operations still presented a challenge. The practitioner-researcher observed from experience that CTI is only useful in environments that accept the need for it and understand how to leverage it. The challenge of getting stakeholders in Greenback Financial to use CTI was twofold. CTI relates to adversaries that are resourceful (e.g., nation-state backed APTs, organised criminals) and simultaneously invisible. As a result, stakeholders perceive threat intelligence to be of a largely speculative nature that is often unable to provide attribution to an attack. Hence when faced with a choice between acting on a speculative piece of intelligence that will incur a cost (reduction of uptime) or not acting on the threat intelligence (i.e., preserving the bottom line), most stakeholders chose the latter. This situation was further exacerbated when threat intelligence appears to be sounding a false alarm. Cybersecurity operations personnel were then perceived to be "crying wolf" which resulted in the erosion of trust between business and IT parties.

If Greenback Financial were to develop cybersecurity risk management practices to enable it to survive in the new hostile environment, then stakeholders would have to fully commit to operationalising CTI into routine processes. The deeply embedded compliance culture presented a challenge to the acceptance of CTI as an essential element of business operations in the cyber-militarised era. The practitioner-researcher recognised that although CTI had been successfully adopted in its IT Operations Division, CTI had to be fully integrated into enterprise-wide processes in order to transform the firm's cyber defence behaviour.

3.3.2. Internal survey: enterprise CTI requirements and business culture

The practitioner-researcher commissioned an internal survey. The purpose of the survey was firstly to expand on particular needs relating to CTI driven solutions and secondly, to assess the magnitude of the challenge related to the integration of CTI across the enterprise. Thus a survey instrument was designed to (1) identify CTI needs across different areas of the enterprise, (2) assess the applicability of CTI to various roles (executives, business managers, operational managers) and the extent to which these stakeholders were confident in the utility of CTI in their routine activities, (3) measure the extent to which stakeholders cared about particular cybersecurity outcomes, and (4) assess the level of satisfaction with the existing CTI and the value it provided to them.

The survey instrument was administered to 231 consumers of internal cybersecurity services. The sample was not random, nor blindly selected; instead it was directed at stakeholders who engaged with security teams on CTI in the recent past. Of the 231 surveys sent out, 93 responses were received (Executives: 2; Senior Management: 9; Management: 17: Operational roles: 65). The practitioner-researcher recognised the risk of potential bias, should he conduct the analysis himself (cf., Iversen et al., 2004 on separating different roles of an action researcher to address impartiality). As such, the analysis of the survey data was done by an independent team in the organisation.

The survey results revealed a number of new insights. On average, the more senior a respondent was, the lower their confidence expressed in CTI. Further, stakeholders reported spending considerable time and effort interpreting or making sense of CTI rather than using it. This finding was consistent with stakeholders at all levels expressing concerns with conflicting, fragmented and/or incomprehensible CTI leading to poor utilisation in the important practices of prioritisation and planning.

The findings also suggested that executives were largely unaffected by CTI primarily because the content rarely reached them. Managerial roles were more likely to report higher levels of confidence in CTI, more likely to use it in their planning, and less likely to report major conflicts in work expectations because they received tailored intelligence products with a close fit to their deliverables. In fact, managerial roles were also more likely to report favourable experiences with CTI if their work was short term/tactical in nature and required information that can be actioned immediately, for example, incident response. Managerial roles were less likely to report favourable experiences with CTI if their work was long term/strategic in nature and required information in need of extrapolation, or contextualisation such as strategic forecasting.

Operational roles expressed the most confidence in CTI, but their level of confidence varied depending on the source of the CTI. Operational personnel reported higher confidence in structured intelligence-sources (e.g., vulnerability scanning), which was presented in a consistent format month-on-month, and lower confidence in unstructured data (e.g., CTI advisories). Aligning with this, operational roles were more likely to use this data in their day-to-day operations because of the available detail. This, however, did not translate into any strategic or planning activities, as these typically did not apply given the scope of their operational responsibilities.

The analysis revealed that many stakeholders reluctantly engaged with CTI staff and processes out of obligation. This was at odds with the emerging cyber threat landscape that demands an engaged "combatant" rather than a bureaucratic "compliant" mindset. Clearly, any CTI solution would require a parallel behavioural change process to enlist these "reluctant combatants". This socio-cultural insight became the basis for both solution development and enterprise-wide integration.

3.3.3. CTI solution development & integration

To summarise, the survey revealed that CTI was difficult to consume from the recipients' perspective (Problem 1); CTI did not reach all recipients e.g., executive consumers (Problem 2); CTI had operational utility, but lacked strategic utility (Problem 3); and, CTI consumption was driven by obligation, not as a business imperative (Problem 4).

In response, the practitioner-researcher developed and formalised four design principles to guide integration of CTI across the enterprise. These four design principles map to the nine quality attributes of threat intelligence (refer Literature review, and Figure 3):

3.3.3.1. Consolidated and consistent. Threat Intelligence must be multi-source (to achieve *Accuracy and Precision*), vetted (to achieve *Reliability*), and consolidated (to achieve *Completeness*) prior to release; this approach must be systematic and consistent (to address Problem 1).

3.3.3.2. Centralised and unified. Threat Intelligence functions must be centralised and standardised (to achieve *Accuracy* and *Precision*) to reduce conflicting accounts of threats (to address Problem 1).

3.3.3.3. Responsive, timely and targeted. Threat Intelligence and responsive actions must have clear points of distribution (to achieve *Relevance*) and delivered prior to contingent decisions (to achieve *Timeliness*) (to address Problem 2).

3.3.3.4. Accessible and pre-analysed. Threat Intelligence must be presented as a consumable deliverable that is *Usable, Tailored* and *Predictive* (to address Problem 3 and to some extent Problem 4).

Based on the survey, the practitioner-researcher realised that if the enterprise were to leverage CTI to best advantage, it had to be provisioned in such a way that stakeholders would be motivated to use it by a business imperative linked to their self-interest. Thus, the practitioner-researcher decided that stakeholders had to be acclimated to adversarial environments where they would be compelled to consume CTI to ensure their cybersecurity. Further, the ramifications of ignoring CTI had to be felt. Hence the existing provision of CTI aimed at fulfiling general compliance obligations was terminated. Instead, cybersecurity began to conceptualise CTI-as-a-service to the enterprise, built to meet the needs of its stakeholders – the reluctant combatants – while also advancing cybersecurity's objectives.

CTI-as-a-service encompasses the original military intelligence principles of what makes intelligence valuable and actionable to an organisation (Figure 3). CTI-as-a-service represents a novel practical approach to embodying both CTI as an innovation and incorporating a socio-cultural change element across the enterprise. Internal services are already well understood by commercial managers (as consumers of such services). The concept of CTI-as-a-service draws on prior information systems research that have approached the delivery and support of complex technical phenomena for business users in the form of a service (Scheepers, 2006; Weill & Broadbent, 1998). For example, Weill and Broadbent (1998) illustrate how enterprise-wide IT infrastructure can be considered as a suite of services encompassing people, processes, and technology. The benefits of a service approach include broader engagement with business and understanding of technology phenomena delivered as services.

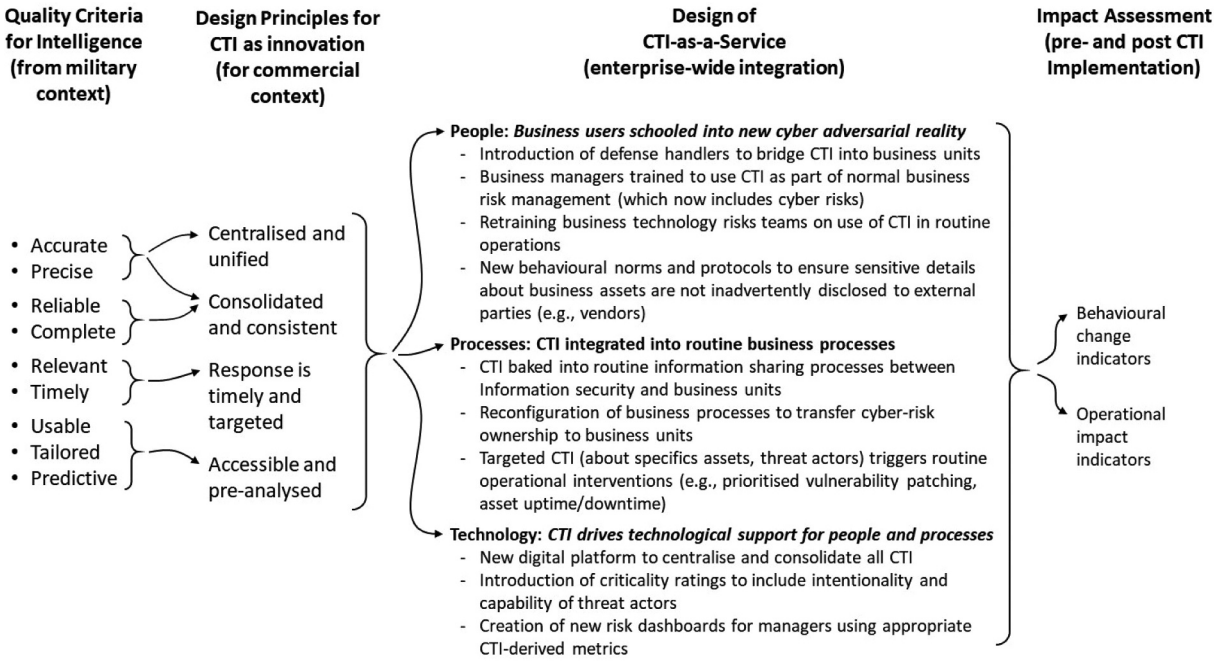

Figure 3. Design principles and impact assessment of CTI-as-a-service.

3.3.3.5. People. From the survey, it was clear that business users would need support to effectively engage with CTI-as-a-service. Greenback introduced a number of specialist CTI managers (or "handlers") recruited from the defence industry whose primary task was to support the needs, context and priorities of CTI business users and direct the existing collection and analysis of CTI to ensure the outcome was *accessible and pre-analysed* to meet their operational and strategic needs.

3.3.3.6. Processes. Re-configuration and re-engineering of processes were needed to: (1) transfer cyber-risk affecting business areas to the responsible business managers, (2) re-task criticality ratings in enterprise risk management processes to incorporate intentionality of threat actors, (3) scale up internal CTI processes to include distribution beyond IT operations, and (4) integrate with business risk teams so consumers would receive CTI that was *consolidated and consistent* with routine business risk reporting.

3.3.3.7. Technology. A new digital platform was needed to *centralise and unify* all CTI. This single platform would replace a number of standalone systems that previously generated CTI reporting largely on an ad hoc basis from various teams (e.g., penetration testers, incident responders, threat intelligence analysts).

CTI-as-a-service was developed as follows. Criticality ratings used to identify and prioritise the severity of risks to specific environments were re-tasked to include intentionality (of cyber threat actors). Intentionality was measured in terms of the capability of a particular threat actor, the perceived attractiveness of the asset to the actor, and the level of exposure of the asset to the actor. This called for novel enterprise-wide risk modelling across organisational systems and assets, including the creation of new risk dashboards for managers and development of appropriate metrics. Importantly, in this process CTI end-users (both operational and managerial staff) were trained in using these resources to support their threat-based decision making. By integrating threat intelligence with routine business risk reporting, the ramifications of ignoring this intelligence was realised by business stakeholders. Effectively, CTI-as-a-service became the vehicle for transferring cybersecurity risks previously owned by the cybersecurity function, to managers responsible for areas affected by these threats. The combination of new risk modelling and dashboards as well as training for designated enterprise stakeholders addressed the need for CTI to be responsive, timely and targeted in the form of CTI-as-a-service. Table 1 summarises details of the service, service level agreements, support and resourcing.

3.3.4. Implementing CTI-as-a-service across the enterprise

The practitioner-researcher observed that although the alerts and advice from the threat intelligence team played a critical role in the IT operations unit's situation awareness of the threat landscape and response to organised, persistent and sophisticated cyber-attacks (refer Figure 2), true cyber resilience requires agile cyber defence across the enterprise. Hence enterprise-wide

Table 1. CTI-as-a-service (Outputs, service level agreements, support and resourcing).

Output	Service Level Agreements	Support Service	Resourcing
Situation Awareness Report (via digital platform)	• Timing: Issued once per week • Evaluation of reliability of source: (e.g., completely reliable, fairly reliable, unreliable, reliability can't be judged) • Level of Confidence in intelligence report: (e.g., confirmed by multiple sources, probably true given other contextual reports, truth cannot be judged)	Defence Handler as interpreter/ advisor	Consumed by business managers, paid for by Cyber security
Flash report (via digital platform)[2]	• Issued no more than 4 hours after a significant event; accompanied by internal evaluation of the reliability of the source and level of confidence in the intelligence • Evaluation of reliability of source: (e.g., completely reliable, fairly reliable, unreliable, reliability can't be judged) • Level of Confidence in intelligence report: (e.g., confirmed by multiple sources, probably true given other contextual reports, truth cannot be judged)		
Personalised Briefing to elaborate on client's risk exposure	• Timing: On demand	CTI team, Private Intelligence Consultan	

business operations must be reconfigured and re-engineered to integrate or "bake" CTI into routine processes (Davenport & Prusak, 1998; Grover et al., 1995; refer "Processes" in Figure 3).

As part of implementing CTI-as-a-service, specific enterprise stakeholders were targeted (refer "People" in Figure 3), given the need to better engage business users (as highlighted by the survey):

3.3.4.1. Business technology risk teams. Business technology risk teams were equipped with intelligence, risk dashboards and were familiarised with CTI terminology (refer "Technology", in Figure 3). These teams were given a detailed walkthrough of the proposed development of CTI-as-a-service. Risk teams were introduced to the threat-intelligence driven view of risk management and review. Given the new modelling, risk teams were required to conduct an immediate review of all previous risk exemptions for cyber-related vulnerabilities if the vulnerability in question was being targeted by a known cyber-threat actor.

3.3.4.2. Business unit managers. The introduction of dedicated defence-trained "handlers" assigned to support business unit managers (refer Table 1) was a critical part of the necessary transformation of the commercial culture. In addition to understanding the needs, context and priorities of these managers, the handlers provided much needed education about the nature of CTI, how it is generated and how to use CTI-as-a-service (and associated digital platform). The development of the relationship between CTI providers and users occurred iteratively. Users could express unmet requirements and areas for improvement in the service. As this practice was routinised, additional alerts and reporting were added to the service. Effectively, various business operations were being reconfigured to better leverage CTI.

3.3.4.3. Executive groups. Executives and senior management were provided with demonstrable proofs of value of the intelligence-driven approach. Following the socialisation work between business and technology risk teams and business unit managers, executive groups were introduced to the enhanced visibility presented by CTI-as-a-service.

3.4. Reflection and evaluation

An important aspect of the action research cycle, with particular relevance to clinical research, is to "reflect on the experience and record learning" (Iversen et al., 2004). At the time of writing this study, there was no single inclusive framework in the formal literature that could be used to benchmark and reflect upon the organisational adoption and integration of CTI-as-a-service as described in this clinical study.

In considering how to measure the impact of CTI implementation on cybersecurity performance, it is useful to revisit the role and function of CTI in organisations. CTI is fundamentally information that has been subjected to a formal process of collection and analysis with the precise objective to inform decision-makers about specific threats, risks and opportunities. Given the role of CTI is to make the cybersecurity behaviour of the firm "proactive, anticipatory and dynamic" (Shin & Lowry, 2020, p. 6), without CTI, the firm is unaware of the who, what, when, how and why of the attack and the threat actors. As a result, their response can only be reactive, and they must assume the worst-case scenario. With CTI, the firm is able to "engineer more precise defense strategies" (Shin & Lowry, 2020, p. 1).

Therefore, given the role and function of CTI in organisations, our study reflects the following logic. Cybersecurity performance is lowered by reactive and undirected defensive behaviours. This clinical study

demonstrates how CTI can be successfully adopted and integrated as a means to transform the organisation's defensive behaviour from being reactive and undirected to being proactive and directed (refer Appendix A). As a result of the behavioural transformation, we found evidence that cybersecurity posture becomes stronger (refer Appendix B).

We provide evidence of behavioural transformation driven by CTI implementation. This shows that the organisation has successfully transitioned its behaviour from being reactive and undirected to being proactive and directed (refer Appendix A, Tables A1, A2). For example, a strong indicator is a distinct shift in the amount of time invested by incident responders from the late phases of the kill chain ("putting out the fire") to the early phases of the kill chain ("preventing the fire from starting"). A second strong indicator is the change in incident response behaviour, from being undirected to directed. A third indicator is discovery of previously unknown vulnerabilities or attack surface that is exposed to cyber-attack.

While we argue that there is no direct causal link between CTI implementation and cybersecurity performance, changes in the indicators (refer Appendix B, Tables B1, B2) suggest a significant impact which could not be realised in the absence of effective CTI implementation. Table B1 provides qualitative measures for the positive impact of CTI implementation on the firm's response to purposive and malicious cyber-threat actors using five operational indicators. Table B2 describes comparable actual scenarios, pre-CTI implementation and post-CTI implementation. Taken together these scenarios demonstrate that the firm has indeed transformed its response from being reactive (and acting on the worst-case scenario) to being proactive and pre-empting the attack. These scenarios are reflective of the organisation's improved response against purposive and malicious threat actors.

Based on the evidence of behavioural and operational impact (as summarised in Table 2), our overall evaluation of the adoption and integration of CTI at Greenback Financial is that it has significantly and measurably improved the organisations cyber security posture.

4. Discussion and conclusion

This clinical study illustrates how military intelligence principles can be adapted and packaged in a form that is suitable and applicable to the commercial context. We believe the essence of Greenback's journey, notably the way that CTI was initially adopted in their cyber security function (Figure 2), then subsequently adapted as an innovation in the form of CTI-as-a-service for enterprise-wide implementation (Figure 3), is transferable to similar commercial organisational contexts. Importantly, this study provides a comprehensive description of the clinical practice to transition from a reactive and undirected response rooted in compliance towards precise defensive strategies driven by threat intelligence. A transition of this magnitude is inherently socio-technical in nature, encompassing not only CTI as technical innovation, but its ripple effect on the rest of the business, operational processes, functional relationships, and behavioural change and ultimately manifests in improved cybersecurity posture. As illustrated in this clinical case, progress on this journey should be assessed on a number of measures, reflective of this social-technical change (refer Appendix).

The study makes the following specific contributions to clinical practice. First, the approach whereby CTI as innovation is initially adopted and implemented within cyber security operations (Phase 1), and is subsequently integrated across the organisation (Phase 2) denotes a useful stage-based roadmap for the deployment CTI in commercial organisations.

Second, CTI-as-a-service represents a novel solution to package and customise generically sourced cyber threat intelligence in a form that can be disseminated and acted upon by specific business units. This allows for customisation of the service for particular business areas, even for specific managers, enabling and training them to prioritise and act upon specific threat intelligence more effectively, compared to the former compliance-driven model. Moreover, accompanying service support (defence-trained handlers, centralised digital platform), adds efficiency in delivering the service that is part of routine business operations.

Third, as cyber security is increasingly pertinent to many organisational processes and activities, CTI-as-a-service can be further scaled up and extended in line with organisational strategies, geographic expansion and emerging cyber threats. CTI-as-a-service is a mechanism to integrate the cybersecurity function (as providers) and business users (as customers). Given the inherently speculative nature of threat intelligence, on occasion, business managers will be called to act upon false alarms. Mutual understanding, trust, and respect is central to this increasingly important organisational relationship (thus the inclusion of personalised briefings as part of CTI-as-a-service, refer Table 1). In turn, this implies that organisations' cybersecurity functions must also transform – becoming central to business operations and strategic planning, as opposed to a back-office function.

Last, the study also contributes to information security risk management theory. The traditional compliance-driven view of cyber security is rooted in probabilistic thinking that focuses on *likelihood* and

Table 2. Evidence of the impact of CTI adoption and integration on cybersecurity defence behaviour (Refer appendix for details).

	Adoption of CTI as Innovation	Integration of CTI-as-a-Service
Summary of Behavioural Impact (refer to details in Tables A1 & A2)	• Shift in distribution of time spent by cyber defence from end stages to early stages of kill chain • Increase in incident response resolution rates • Reduced dwell time of threat actors • Improved consistency in response to cyber attacks • Improved coherence of response activities against cyber attacks	• Increased speed and prioritisation of vulnerability resolution across business assets • Improved knowledge of the vulnerability of critical business assets through the breakdown of CTI-business silos • Improved fusion of CTI and business intelligence leading to improved cyber risk management of business assets • Improved strategic assessment of business opportunities through CTI insights into APT behaviour • Improved effectiveness of routine CTI workflows through incorporation of business stakeholders
Summary of Operational Impact (Pre-CTI Implementation to Post-CTI Implementation) (refer to details in Table B1)	• Disruption to IT Infrastructure Services (Medium-High to Low-Medium) • Attack Surface defended (Unknown to High) • Number of Previously Unaddressed Critical Incidents (Very High to Low) • Effectiveness of Incident Response (Cost/Performance) (High to Low) • Speed of Response (Low to High)	

impact as means of prioritising interventions and quantifying risk reductions. We argue that in the case of purposive threat actors, cyber-security risk is not probabilistic but possibilistic. Organisations should realise that possibilistic cyber-risks are inherently unpredictable and there is no determinate relationship between investment in security safeguards and reduction in risk exposure. To address possibilistic cyber-risks, organisations must introduce two new externally focused constructs, i.e., cyber-threat actors' *intentionality* and *capability* into their risk calculus.

An externally-focused risk calculus is better suited to the emerging cyber-threat landscape typified by high volume, sophisticated and targeted attacks. The clinical study describes the experience of an organisation that designed and implemented an enterprise-wide solution, founded on this externally focused risk calculus. CTI redresses the information asymmetry that sophisticated cyber threat actors have over organisations. The practical reality is no longer *if* an attack will take place, but *when (timing)*, by *whom (attacker), why (motive), how (tactics)*, and *where (targets)*. CTI-as-a-service provides managers with critical operational, tactical and strategic information about these questions, enabling them to direct their cyber-defence function against purposive and malicious attacks.

To the best of our knowledge, this clinical study is the first of its kind that demonstrates how a large commercial organisation has adopted and integrated CTI as a means to successfully transform its cybersecurity defence behaviour.

In terms of limitations, for reasons of confidentiality, we were limited in the amount of detail we could provide in this paper. However, the broad approach and solution presented here are relevant to organisations that seek to deploy CTI to defend against cyber military entities.

Notes

1. The organisational context referenced in this paper is the first author's personal reflections on his lived experience in his professional role spanning a number of organisations and does not reflect in any way the posture or position of any of the organisations involved.
2. A threat intelligence alert triggered by an external event (e.g., an attack on another financial organisation).

Acknowledgments

We would like to acknowledge the thoughtful inputs and suggestions received from the reviewers and editorial team on this paper.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

James Kotsias is the Director of Advantage Cyber. He holds a Master's Degree in Information Systems from The University of Melbourne. He leads an offensive security and operations function, and advises long-term cyber security and threat strategy for a number of organizations. James also sits on the Cyber Executive Advisory Board at Deakin University; providing input to the Cyber Security Research and Innovation Center (CSRI) and its extended intelligent systems research. His current research interests are the expanding theater of cyber warfare, the evolution of

corporate espionage, the weaponisation of defensive systems, and kinetic incident response structures. James blue-screened his first PC at the age of 7.

Atif is an Associate Professor at the University of Melbourne's School of Computing & Information Systems where he serves as Deputy Director of the Academic Centre of Cyber Security Excellence. Atif leads a unique team of Cybersecurity Management researchers drawn from information systems, business administration, security intelligence, and information warfare. He has authored over 100 scholarly articles in cybersecurity management and received over AUD$5M in grant funding. Atif is an Associate Editor for the leading IT security journal, Computers & Security. He has previously served as a cybersecurity consultant for WorleyParsons, Pinkerton and SinclairKnightMerz. Atif is a Certified Protection Professional with the American Society for Industrial Security. For more information, please visit https://www.atifahmad.me/

Rens Scheepers is a Professor in the Department of Information Systems and Business Analytics at Deakin University. He also serves as Director of the Business & Technology research theme at the Deakin Business School. His research focuses on how organisations can achieve and protect competitive advantages from the application of contemporary information and communication technologies and systems.

ORCID

Atif Ahmad http://orcid.org/0000-0002-8862-5755

References

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, *86*, 402–418. https://doi.org/10.1016/j.cose.2019.07.001

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 1–15. https://doi.org/10.1016/j.cose.2020.102122

Avison, D. E., Lau, F., Myers, M. D., & Nielsen, P. A. (1999). Action research. *Communications of the ACM*, *42*(1), 94–97. https://doi.org/10.1145/291469.291479

Bank of England. (2016). *Understanding cyber threat intelligence operations*. https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf

Baskerville, R., & Wood-Harper, A. T. (1998). Diversity in information systems action research methods. *European Journal of Information Systems*, *7*(2), 90–107. https://doi.org/10.1057/palgrave.ejis.3000298

Baskerville, R. (2005). Information warfare: A comparative framework for business information security. *Journal of Information System Security*, *1*(1), 23–50. https://www.jissec.org/Contents/V1/N1/V1N1-Baskerville.html

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Bostrom, R. P., Gupta, S., & Thomas, D. (2009). A meta-theory for understanding information systems within sociotechnical systems. *Journal of Management Information Systems*, *26*(1), 17–48. https://doi.org/10.2753/MIS0742-1222260102

Cooper, R. B., & Zmud, R. W. (1990). Information technology implementation research: A technological diffusion approach. *Management Science*, *36*(2), 123–139. https://doi.org/10.1287/mnsc.36.2.123

Crowdstrike. (2021). Threat intelligence: Cybersecurity's best kept secret. https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperThreatIntelligence.pdf

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business Press.

Ettinger, J. (2019). Cyber intelligence tradecraft report: The state of cyber intelligence practices in the United States. Retrieved from Carnegie Mellon University: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=546686

FM 2-0. (2010). *Field manual 2-0: Intelligence*. Headquarters, Department of the Army.

Giles, L. (1910). Sun Tzu on the art of war the oldest military treatise in the world translated from the Chinese is that is fixed. *Sun Tzu On The Art Of War*. Abingdon, Oxon: Routledge.

Grover, V., Jeong, S. R., Kettinger, W. J., & Teng, J. T. (1995). The implementation of business process reengineering. *Journal of Management Information Systems*, *12*(1), 109–144. https://doi.org/10.1080/07421222.1995.11518072

Holland, R. (2015). Forrester.https://www.forrester.com/report/Vendor+Landscape+SR+Pros+Turn+To+Cyberthreat+Intelligence+Providers+For+Help/-/E-RES113066

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Paper presented at the International Conference on Information Warfare and Security*, Washington, DC, USA. Lockheed Martin Corporation.

Iversen, J. H., Mathiassen, L., & Nielsen, P. A. (2004). Managing risk in software process improvement: An action research approach. *MIS Quarterly*, *28*(3), 395–433. https://doi.org/10.2307/25148645

Lawson, C., Contu, R., & Benson, R. (2019). *Market guide for security threat intelligence products and services*. Gartner. https://www.gartner.com/en/documents/3902168

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, *72*, 26–59. https://doi.org/10.1016/j.cose.2017.08.005

McKay, J., & Marshall, P. (2001). *The dual imperatives of action research*. Information Technology & People.

Microsoft Corporation. (2020). *Microsoft digital defense report*. https://www.microsoft.com/en-us/download/details.aspx?id=101738

Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. *Information Systems Journal*, *16*(4), 317–342. https://doi.org/10.1111/j.1365-2575.2006.00221.x

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). Free Press.

Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In: Holt T., Bossler A. (Eds.),*The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, Cham.135–154. https://doi.org/10.1007/978-3-319-78440-3_8

Scheepers, R. (2006). A conceptual framework for the implementation of enterprise information portals in large organizations. *European Journal of Information Systems*, *15*(6), 635–647. https://doi.org/10.1057/palgrave.ejis.3000646

Schein, E. (1987). *The clinical perspective in fieldwork*. Sage.

Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2021). Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, 20, 21–38. https://doi.org/10.1007/s10207-020-00490-y

Schön, D. A. (1983). *The reflective practitioner: How professionals think in action*. Basic Books.

Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the 'cyberthreat-intelligence (cti) capability'that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security*, *92*, 101761. https://doi.org/10.1016/j.cose.2020.101761

Tornatzky, L. G., & Klein, K. J. (1982). Innovation characteristics and innovation adoption–implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management*, *29*(1), 28–45. https://doi.org/10.1109/TEM.1982.6447463

Verizon Corporation. (2018). *Data breach investigations report*. https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44(July 2014)*, 1–15. https://doi.org/10.1016/j.cose.2014.04.005

Weill, P., & Broadbent, M. (1998). *Leveraging the new infrastructure: How market leaders capitalize on information technology*. Harvard Business Press.

Appendix A. Evidence for Improvement in Greenback's Cybersecurity Behaviour

We provide evidence of measurable indicators of impact of both the adoption of CTI (Phase 1, Table A1) and integration of CTI-as-a-service (Phase 2, Table A2), utilising the relevant tradecraft indicators (adapted from a report that contains indicators of CTI use drawn from the practices of 32 US organisations (Ettinger, 2019)). Table B1 provides an operational impact assessment of CTI Impact against five indicators (pre and post Implementation). Table B2 compares actual cyber-attack scenarios on Greenback, demonstrating the impact of CTI (pre- versus post Implementation) on the organisation's cybersecurity posture. Where relevant we have provided the sources of evidence used to construct our measures.

Table A1. Behavioural transformation due to CTI adoption: dealing with new and emerging hostile threats as reality (Phase 1).

State of Greenback Pre CTI Adoption	State of Greenback Post CTI Adoption	Post CTI Adoption: Indicative evidence that CTI adoption is a measurable success in terms of cybersecurity posture	Relationship between CTI adoption and organisational cybersecurity posture	Sources of Evidence
Pre-CTI Adoption Incident Response Behaviour: Firm's cyber defence of business assets was directed by inward views of asset criticality The firm invested disproportionate resources securing top tier assets over less critical assets as it assumed attackers shared the same priorities. As a result, attackers were exploiting vulnerable entry points in less critical assets such as mail servers as they were not actively defended.	**Firm's cyber defence of business assets is directed by a combination of an inward view of asset criticality as well as an outward view of threat actor intent and capability** Adoption of CTI introduced the attacker's perspective of the firm which changed how the firm defended its attack surface. For example, significant security resources were invested in surveillance to combat attacker reconnaissance and guard entry points to prevent penetration.	• Increased effectiveness of response mitigations leading to fewer future incidents downstream • Increase in incident response resolution rates	Adoption of CTI leads to improved alignment between the activities of cyber defence and cyber attack	• Incident Management Records • Risk and Problem Ticketing Records • Risk Registries • Asset Registries • Network Taxonomy Reporting
Majority of time spent in cyber defence was in the late stages of attack operations (e.g., exploitation) mitigating the impact of the attack Prior to CTI, incident response teams were unable to anticipate attacker behaviour. Hence attacks were detected late in the kill-chain.	**Majority of time spent in cyber defence is in the early stages of the attack operations (e.g., reconnaissance) preventing the attacker from reaching their objectives** Integration of CTI enabled response to understand threat-actor objectives and patterns of behaviour leading to detection of attacks in the early phase of the kill-chain.	• Shift in distribution of time spent by cyber defence from end stages to early stages of kill chain • Reduced mean time to incident response • Reduced dwell time of threat actors	Adoption of CTI leads to reduced success rate (and therefore impact) of cyber-attacks as firm halts attack operations earlier rather than later	• Incident Management Records • Risk and Problem Ticketing Records • SLA Tracking via Response Tickets
Majority of the firm's response to cyber-attack consisted of activities that were ad hoc, undirected and unstructured. Without profiles of threat actors and background knowledge on intent, capability and objectives, incident responders wasted time inspecting unrelated logs, misattributing patterns of activity, and making uninformed decisions.	**Majority of the firm's response to cyber-attack consists of activities that are planned, directed and structured** CTI enabled the firm to plan a structured and directed response process with clear inputs and decision points. This allowed downstream functions to perform their role with more focus (rather than individually finding and filling in missing context), resulting in better outcomes along the response chain.	• Improved speed to deployment of resources • Improved consistency in response to cyber attacks • Improved coherence of response activities against cyber attacks • Increased directedness in response to activities of cyber-threat actors	Adoption of CTI leads to improved efficiency and focus of cyber defence operations against cyber attacks	• Risk Registries • Core Process Documentation

Table A2. Behavioural transformation due to CTI integration into the broader enterprise: CTI-as-a-service (Phase 2).

Initiatives to integrate CTI across broader enterprise	Early indicative evidence that CTI-as-a-service is being utilised (measures adapted from Ettinger (2019))	Sources of Evidence	Indicative evidence that CTI integration is a measurable success in terms of cybersecurity posture	Sources of Evidence
People: Introduction of specialist CTI managers (or "handlers") recruited from the defence industry whose primary task was to understand the needs, context and priorities of CTI users and direct the existing collection and analysis of CTI to ensure the outcome was tailored to their operational and strategic needs. **Process**: Re-configuration and re-engineering of processes to enable: (1) transfer of cyber-risk affecting business areas to the responsible business managers, (2) re-tasking criticality ratings in enterprise risk management processes to incorporate intentionality of threat actors, (3) scaling up of internal CTI intelligence processes to include wider distribution points outside of IT operations, and (4) integration with business risk teams so consumers would receive CTI that was coherent and consistent with routine business risk reporting. **Technology**: A new digital platform to centralise and consolidate all CTI. This single platform replaces a number of standalone communication systems that previously generated CTI reporting largely on an ad hoc basis from various teams (e.g., penetration testers, incident responders, threat intelligence analysts).	• Increased speed and prioritisation of vulnerability resolution across enterprise business assets • Improved effectiveness in the utilisation of CTI in business operations • Sustained utilisation of CTI amongst all stakeholders as evidenced by CTI-related activity on digital platform • Improved strategic assessment of business opportunities through incorporating cyber-threat intelligence • Improved knowledge of the vulnerability of critical business assets through the breakdown of CTI-business silos • Improved fusion of CTI and business intelligence leading to improved cyber risk management of business assets • Improved cross-functional collaboration among CTI and business stakeholders enabling improved knowledge of attack surface • Improved effectiveness of routine CTI workflows through incorporation of business stakeholders • Improved identification and tracking of sensitive business data attractive to threat actors (previously not considered)	• Incident Management Records • Risk and Problem Ticketing Records • Risk Registries • Investment Slate Assessment • ROI Differential Analysis	• Integration of CTI leads to reduced enterprise-wide attack surface through increased speed and prioritisation of vulnerability resolution • Integration of CTI leads to reduced cyber-risk exposure due to improved utilisation of CTI across enterprise operations • Integration of CTI leads to increased effectiveness of business strategy due to incorporation of CTI into business risk assessment • Integration of CTI leads to swifter enterprise-wide adaptation to changes in the cyber threat environment	• Incident Management Records • Core Hardware Asset Registries • Availability Metrics • Network Taxonomy Reporting

Appendix B. Evidence for Improvement in Greenback's Cybersecurity Posture

Table B1. Operational impact assessment (Pre and post CTI implementation).

Operational Impact Indicator	Pre-CTI Implementation	Post-CTI Implementation
Disruption to IT infrastructure services	Medium-High	Low-Medium
Extent of attack surface defended	Unknown	High
Number of previously unaddressed critical incidents	Very High	Low
Effectiveness of incident response (performance/cost)	Low	High
Speed of response	Low	High

Table B2. Actual cyber attack scenarios on greenback demonstrating impact of CTI (Pre and post implementation).

The impact of CTI implementation can be seen in a comparison of two near-identical threat responses to two similar vulnerabilities (Vuln-20 and Vuln-21) in an enterprise messaging platform. The responses to each of these vulnerabilities occurred pre- and post-CTI implementation respectively. Both vulnerabilities were assessed at the highest level of criticality.

Pre-CTI Implementation	Post-CTI Implementation
Greenback became aware of active threats exploiting Vuln-20, but was unable to form a consistent view of likely attack surfaces, or points of entry. The eventual direction of the response was informed by a detection of malicious activity in an adjacent environment, which was traced back to use of the exploitation of this vulnerability. The response, therefore, was consistently behind the threat actor – having little reliable knowledge of their modus operandi, or objectives. Unable to pre-empt or keep pace with attackers, Greenback was forced to isolate the affected environments from the broader network; stemming the spread of the threat at the cost of material disruption to enterprise systems and operations.	Greenback was targeted by a similar threat actor, exploiting a similar vulnerability, Vuln-21. Through established channels with peer organisations and private vendors, CTI was able to obtain indicators of compromise (IoCs), logs, IP addresses, signatures, and other technical indicators observed and confirmed as "signals" before a threat actor attempted a full-scale compromise. Having established a credible threat, the cybersecurity function reached out to business teams and asset owners to arrange downtime for mitigations to be put in place. Teams were deployed specifically to defend the assets at risk, and a high-priority response process was used to expedite patching – mitigating the vulnerability entirely. There was no meaningful disruption to business operations, and the attack never proceeded, the attacker having lost the opportunity to establish a meaningful foothold.