Towards the Elucidation of Organizational Cyber Threat Intelligence

Bongsik Shin, San Diego State University, USA
Matthew Levy, Hawaii Pacific University, USA

Abstract

This article details the new and evolving field of Cyber Threat Intelligence (CTI) and offers practical advice for practitioners seeks to add a CTI component to the cybersecurity posture of their organization. To accomplish this, we synthesize literature from academic and practitioner sources to detail the Organizational Cybersecurity Threat Intelligence (OCTI) Model as a way for organizations to think about the many different facets of CTI. The model contains a Threat Analysis component, containing three subcomponents that explain the discovery, detection, and learning components essential to CTI analysis, and also a Threat Response component which explains the adaptation, shaping, and selection components of CTI response. Collectively, we hope this model stimulates the topic of CTI amongst researchers, and that it stimulates the idea of Cybersecurity organizations getting to know more about the behavior of their adversaries.

Introduction

Cybersecurity threats are entering a new dawn. We already know the intensity and frequency of security breaches has reached new levels, as far more sophisticated malware, social-engineering, and statesponsored cyberterrorism is now occurring at unprecedented levels. For example, we have significant reason to believe Russian hackers infiltrated the computers of the Democratic National Committee, resulting in four different congressional investigations of Russian meddling in US elections. We have significant reason to believe computers with Chinese IP addresses were connected with the infiltration of three department networks and the stealing of classified information in Canada. We have significant reason to believe the United States played a major role in the proliferation of the Stuxnet worm that penetrated Iranian-based Windows computers used to control nuclear-weapon-producing machinery. And we have significant reason to believe that governments are not the only ones affected, as, for example, Operation Aurora, a cyberattack connected to the Elderwood Group based in Beijing with known ties to the People's Liberation Army, took aim at companies such as Google, Adobe, Juniper Networks Northrup Grumman, Rackspace, and many others.

Interestingly, the tools of the adversary are, many times, not that complex. They are simple, 'off-the-shelf' tools, that focus on exploiting the human element as opposed to solely exploiting technology. So, it's not just the ones and zeros part of an attack that's sophisticated. It is the development of sophisticated psychological exploitations to find little known weak points within an organization. As alluded to above, this is being undertaken by criminal organizations, as well as nation states, and is nearly indistinguishable in terms of the time and quality it takes to manifest an attack. The question now is not what more can be done to harden networks, but what can be done to become better acquainted with an organization's adversaries?

Viewing this, a new field has emerged under the auspices of Cybersecurity called Threat Intelligence that deserves attention from both researchers and organizations. Currently, this field is new, chaotic, and widely dispersed. Data feeds originate from numerous corporations and government agencies about threats, and numerous data standards are available for processing threat data. In addition, organizations also lack a clear way to form a strategy for an organizational threat intelligence capability, making an appropriate basis for gathering, contextualizing, and acting upon pertinent threats an elusive task. In our current cyberreality, it is impossible to corral and act upon every threat from every intelligence feed. It

also impossible to deploy every machine-learning algorithm at our disposal. Thus, organizations need a way to think, balance, strategize, and score threats, and their appropriate responses.

This article provides a model for Organizational Cyber Threat Intelligence, hereafter referred to as the OCTI model. To accomplish this, we draw from academic and practitioner research in the areas of Cybersecurity and Threat Intelligence to elucidate the model. This helps elucidate an organizational framework for people, processes, and technology that augment existing cybersecurity measures with a threat intelligence component. In this regard, OCTI is not just representative of the outer layer of a defense-in-depth strategy (NSA, 2015), but a way to approach the topic of threat intelligence, and to inform and target the efforts of those focusing on cybersecurity in an organization.

Background

CTI represents threat information primarily about cyber adversaries, which is timely, context-oriented, evidence-based, analytical, and specific; and thus, actionable and can aid decision-making (Holland, 2013; Johnson et al., 2014; Townsend et al., 2013). Strictly speaking, the goal of CTI is to drive activities that gather information about potential adversaries. In this regard, CTI spans three temporal dimensions: past, present, and future, and should represent a framework for an organization that facilitates the identification of previously unknown threats and vulnerabilities in the following ways: through the lens of historical incidents, through prioritization in countering active threats, and through the monitoring and prevention of repeat attacks. Accordingly, CTI can be oriented towards the following: anticipatory future intelligence or evidence-based intelligence (Coyne et al., 2014); strategic-, operational-, tactical-, or technical-level intelligence (Chismon & Ruks, 2015; Poputa-Clean, 2015), and/or atomic, computed, or behavioral intelligence (Hutchins et al., 2011).

Presently, research in academic and practitioner literature points toward a lack of balance between the knowledge an organization has about the protection of its own assets versus knowing about the assets, capabilities, and behaviors of potential adversaries (Holland, 2013; Johnson et al., 2014; Townsend et al., 2013). And we take this to signal that research and practice could greatly benefit from guidance that looks deeply into the threat intelligence phenomena in organizations, so as to develop analytic frames and practically-oriented frameworks. Sun Tzu, and his treatise, The Art of War, couldn't have said it any better:

> *"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" (Giles, 1910, p. 52).*

Presently, much of what is researched in the cybersecurity literature points towards knowledge of oneself, with much less focus on the enemy. We contend this leads to research that, erroneously, informs practice towards a cycle of victories and defeats. The crux of the problem is that effective defense solutions are still reactive by their very nature (Ghernouti-Helie, 2010), as instead of focusing on way to become more acquainted with the tendencies of adversaries, research has centered on effective ways to fix vulnerabilities (Chen et al., 2016), detecting when breaches occur (Dhillon, 2015), and the use of signatures such as mutexes and other indicators of compromise amongst one's own organizational assets (Vanderpol et al., 2010).

Reasons for this type of security posture vary widely, but one that sticks out is that compliance still plays a key role (Susskind, 2014; McBride et al., 2012). In addition, research has also placed significant emphasis on the micro-, meso-, and macro-behaviors related to compliance and policy requirements (Karjalainen and Siponen, 2011; Ramachandran, et al., 2013), choosing to focus on research studies that deal with risk management and mitigation, and compliance behavior as a way to find and neutralize potential threats (Zafar and Clark, 2009). In contrast, research that looks at a cybersecurity from an anticipatory and preemptive manner has received much less attention (Muckin & Fitch, 2015).

From the perspective of the practitioner, extant risk modeling methods and frameworks are largely aligned with a defense-driven know yourself process. For example, the Operationally Critical Threat,

Asset, and Vulnerability Evaluation (OCTAVE) framework is focused on creating profiles of critical information assets. The Open Web Application Security Project (OWASP) is focused on improving the security of an organization's software assets. And even though the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) framework is focused on threat modeling, it is focused on internal threat knowledge and finding internal threats to that system, e.g. 'what can go wrong with the system being worked on', whilst paying little attention to facilitating proactive understanding of threats and enemies, germane to a particular organization.

Along with many others, we contend that balancing the efforts of knowing one's own capabilities and knowing the capabilities of one's adversaries is critical for the security posture of the modern organization (Muckin and Fitch, 2015; Miles, et al., 2014). Despite the initial investment, we contend CTI is important for organizations for the following reasons: Research has shown that many attacks are in the category of APTs (Advanced Persistent Threats). Moreover, such attacks are inflicted by well-resourced criminal organization and even rogue states. Lastly, in order to fend off APTs, traditional defense measures centered on a 'know yourself' philosophy is practically infeasible (NTT, 2014).

The threat frontier is just too broad to be effectively covered by traditional, generalized defense methods. There is a need for an organization to determine threats and vulnerabilities particularly relevant to its own internal and external business environments for pre-emptive deployment of tailored defense. This requires heightened situational awareness of the threats, threat actors, their targets, their capabilities, as well as target profiles (e.g., assets, data) and their vulnerabilities. Improved situational awareness through a CTI program can greatly facilitate the customized and thus more effective planning of countermeasures and mitigation control, curtailing risks by avoiding blind flights in its journey through the cyber mine fields. The theory of counterintelligence (Prunckun, 2014) implies that the countermeasures and mitigation controls can be in three different categories: deterrence (or obstruction) of threat exercise by adversaries; neutralization to block intelligence gathering or to cause loss of interest in carrying-out threat operations; and deception to mislead threat actors.

Accordingly, we analyzed the literature in research and practitioner articles to develop a threat intelligence model for organizations. We develop two major components of Threat Analysis and Threat Response for the OCTI model, with 6 major subcomponents under each of these categories.

The OCTI Model

OCTI can be understood in terms of two high-level capability dimensions: threat-analysis and threat response capabilities. An organization's threat-analysis capability is comprised of three components: discovery, analysis, and learning capabilities, while an organization's threat response is comprised of an additional three components: adaptation, shaping, and selection capabilities. Figure 1 illustrates the OCTI Model

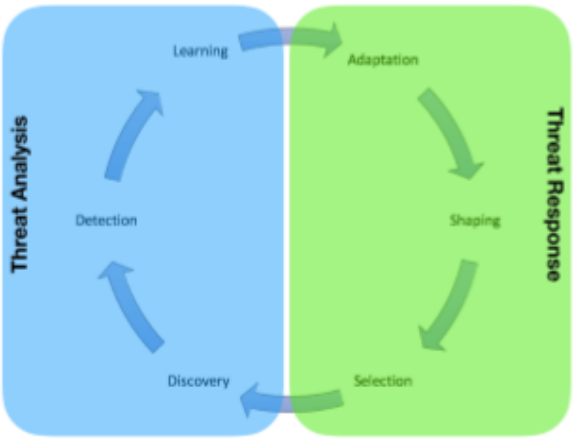

Figure 1: The OCTI Model

The Threat Analysis Capability

Threat Analysis requires the organization to understand the potential actions of its adversaries. While the efficacy of a threat analysis capability in an organization might be difficult to measure, it can be seen in terms of the actions it produces to analyze external threats and produce new actions to secure organizational assets. These are actions that might not have otherwise occurred through a 'know yourself' examination of one's internal assets alone. Thus, a Threat Analysis capability in an organization looks at the potential actions of adversaries, and can be broken down into the following components: investigation of the discovery of adversaries' potential actions, the ability to detect the real-life credibility of external threats, and the organizational learning that builds knowledge about the capabilities of adversaries. Moreover, a Threat Analysis capability is context-sensitive. It must be contextualized to the types of assets the organization needs to protect, and/or the type of industry the organization finds itself in. The following three sections describe the three Threat Analysis capabilities of discovery, detection, and learning.

Discovery Capability

Essential to OCTI is the ability to have an organizational capability that fosters the discovery of new information about the threats of potential adversaries. In particular, an organization must have the ability to discover threats relating to both internal and external environments as a comprehensive threat landscape, but at strategic, operational, tactical, and technical levels in order to derive CTI requirements of an organization. Research has pointed to the importance of leadership integration in a discovery capability (Bhatt et al., 2014), as leadership integration is critical for the threat intelligence team to be able to quickly obtain necessary resources, and achieve better return on investment (Townsend et al., 2013).

Also, essential to a Discovery Capability is that it originates from a 'know yourself' position and is contextsensitive to the mission of the business. Organizations must have a grasp of critical assets (e.g., business assets and security assets), be able to create asset profiles to appropriately define the "attack surface" (Muckin & Fitch, 2015) which facilitates the organization's the ability to decompose potential target systems. Specific activities relevant to identifying critical assets and creating asset profiles include, but are not limited to, the creation of an asset rule base (e.g., asset dependencies), determining asset values as a function of confidentiality, availability, and integrity, and creating specific asset profiles and rules for data, hardware, software, networks, procedures, and asset configurations tailored to asset values. To define the attack surface, the internal target surface may be defined in terms of applications, systems, and enclaves (e.g., subnets) that directly or indirectly communicate with or provide access to the assets that need protections. The applications, systems, and environments need to be decomposed and evaluated in both managerial (e.g., existing policy and security controls, associated service and management functions) and technical details (e.g., communication protocol, application programming interfaces). Also, some of the most serious threats are from insiders with malicious intent (e.g., altering or hiding information to hamper decision-making). Thus, there are conditions conductive to internal threats (e.g., excessive access privilege, weak data management policies & procedures) that must be accounted for (Costa et al., 2016) and techniques such as behavioral modeling (Cole, 2014; Santos et al., 2008) may be used to assess the internal threat surface. Accordingly, much of the internal discovery efforts overlap with the traditional vulnerability/risk management practices in an organization, and can be viewed as their natural extension.

In sum, discovery entails an organization be aware of the external threat landscape by identifying critical assets, and using this information to follow potential adversaries through threat feeds and the dark web in order to understand how their tactics, techniques, and procedures (TTPs) evolve over time (Townsend et al., 2013). Some of the key discovery components available to industry today include the following: threat trend reports and feeds, publicly available profiles of threat actors and their TTPs, publicly available vulnerability reports, intrusion or network attack vectors, tools profiles used by adversarial actors, and publicly available information that might negatively affect an organization's services or products. Profiles

of adversaries can include such information as malware and attack tools used, command and control infrastructure, spear-phishing TTPs, common targets, motivations, and profiting methods (Irwin, 2014).

Detection Capability

Detection of internal and external threats, threat sources, and threat actors is particularly relevant to the overall security posture of an organization (Prunckun, 2014), and thus, constitutes the core of OCTI. Both strategic and functional-level findings in the discovery stage and subsequent derivation of OCTI requirements become critical inputs to the detection phase to better structure CTI efforts and to ensure adequate scope management by committing adequate amount of business resources and gathering right amount of data necessary to perform meaningful analysis. Once CTI requirements are in place, the analytical procedure can follow through the general steps of: determination of data sources, determination of access methods, data gathering/aggregate/sharing/analysis platforms, internal and external gathering of data (e.g., gather vulnerability data, agglomerate threat data), processing of raw data (e.g., enrich data points, data fusion), data analysis (e.g., correlate vulnerabilities and threats with assets), and CTI dissemination (e.g., Holland, 2103; Los et al., 2014).

Presently, there are a number of data sources for CTI detection efforts for the cybersecurity-aware organization. From an internal, 'know yourself' perspective, firewall logs, intrusion detection/prevention systems, anti-virus alerts, OS and application logs are seen as critical detection mechanisms (Johnson et al., 2014; Fransen et al., 2015). From an external perspective, the cybersecurity aware organization can ingest data from places such as honeypots, known decoys, open source intelligence (OSINT) sources such as AlienVault or the Facebook Threat Exchange, business partners, and other forms of human intelligence (HUMINT) such as product vendors, law enforcement agencies, and agencies such as InfraGard and the European Network and Information Security Agency (ENISA).

The aforementioned sources represent various types of detection related threat data. For example, information can be gathered about threat actors, malware indicators (e.g., attack signatures, hash values), IP reputation data (e.g., adversary networks, blacklisted addresses), URLs and domain names, command and control networks (e.g., botnets), phishing sites/messages, network/host artifacts, attack tools, and TTPs (Los et al., 2014; Securosis, 2015). Accordingly, they become actionable intelligence through analysis (e.g., correlations) and assessment in terms of threat vectors, vulnerabilities, threat actor types and adversary profiling, anticipated risks, and effects of successful attacks (Irwin, 2014; Kime, 2016). In this regard, the 'Pyramid of Pain' model (Bianco, 2013) can also serve as a useful guide. Not only does it suggest various intelligence types derived, as well as their potential usefulness, but it also indicates difficulties of obtaining such intelligence. One key element of this phase is the use of ratings systems. For example, rating threats based on impacts (e.g., benign, medium, critical) or confidence (e.g., unknown, low, medium, high). In addition, existing ratings systems, such as the CVSS (Common Vulnerability Scoring System), CWSS (Common Weakness Scoring System), and the SANS Confidence Matrix (Poputa-Clean, 2015; Townsend et al., 2013) can be useful in this regard. In sum, when an organization can implement a tiered threat model in which threats can be ranked and prioritized on a regular basis in terms of their severity and potential targets of threat actors, its CTI program becomes more effective (Townsend et al., 2013).

Learning Capability

As a critical OCTI component to Threat Analysis, organizations should also actively engage in learning to help turn itself into a 'cognitive enterprise' that continuously learns and creates knowledge, as this is an important condition for business success (e.g., Argote & Miron-Spektor, 2011). Organizations cannot simply buy CTI capability, for example, in the form of learning algorithms or threat data feeds. It has to be gradually built and cultivated over time through continue practices, knowledge acquisition, and growth in CTI maturity during the discovery, analysis, and post-analysis phases (Holland, 2013). Research has explicated that an organization with a mature threat/vulnerability lifecycle management process can reduce remediation time, while its absence can increase greatly increase susceptibility as many as four times as much (NTT Group, 2014). What this means for the learning component of OCTI is that, first, an organization should be explicit about how it learns from past threats and incidents in order to ensure they

do not fall victim to similar threats or incidents. Second, threats and threat sources are highly dynamic moving targets, propagating much faster than the organization's ability to react (Archer & Wick, 2013), and thus, organizations should cut the speed gap through continuous learning. Third, organizational learning should augment capability in curtailing the rates of CTI false positives and false negatives an organization inevitably faces (Securosis, 2015). This way, an organization can successfully prevent the CTI noise from wasting corporate resources and distracting frontline workers from focusing on real dangers. Fourth, an organization should be able to automate information processing even for unstructured security functions by re-applying existing knowledge. Fifth, organizations may be best served by implementing learning through sharing. This is a hugely important success condition of CTI, as it is important to foster a culture culture of active inter-organizational CTI sharing, especially as cyberattacks target multiple organizations, oftentimes in the same industry segment (Chismon & Ruks, 2015; Johnson et al., 2014; Muckin & Fitch, 2015; Ring, 2014; Townsend et al., 2013). An organization can reach the highest level of maturity in managing cyber risks when it actively shares CTI and engages with external communities, rather than just consuming information provided by others (NIST, 2014). Such organizational learning through interorganizational CTI sharing manifests its benefits in various manners including elevated situational awareness, better understanding of threats, augmented defensive agility, and improved decision making (Johnson et al., 2014). To facilitate information sharing, CTI sharing can take the form of centralized (or hub-and-spoke), peer-to-peer, or hybrid architecture (Johnson et al., 2014), each with own strengths and limitations.

CTI, uncovered, serves to effectively augment the 'know yourself' defense system's learning so that it reduces repeated investigations triggered by similar false alarms (Bhatt et al., 2014). Some of the advanced learning functions include creation of a baseline of 'normal' activity of the environment, prioritization of threats and alerts, management of overlaps in intelligence feeds, searchability of CTI data sources and flexible scoring mechanism of urgency (e.g., red/yellow/green), and relevance determination of intelligence from different angles including attack surface, reliability, or usefulness of intelligence feeds.

Despite the critical nature of CTI sharing and continuous advancement of sharing platforms (e.g., STIX) (Barnum, 2012; Holland, 2013; Securosis, 2015; Shackleford, 2015), behavioral, psychological, economic and cultural barriers (Chismon & Ruks, 2015; Hsu et al., 2012; Ring, 2014) keep many organizations from being proactive, and timely, in the sharing of threat information. It may be that there appears to be a lack of motivation and 'social' infrastructure to support learning about CTI in organizations. It may be that organizations appear to have the implicit belief that they have nothing of value to share. It may be that many organizations harbor a lack trust about sharing with other organizations in their competitive space, or that organizations may not be clear on what to share (Chismon & Ruks, 2015). Lastly, it may be that organizational culture may not be conductive to sharing even in particularly large organizations such as government agencies and the finance sector (Hsu et al., 2012; Townsend et al., 2013).

To summarize, the threat analysis component of the OCTI model emphasizes that organizations possess a discovery capability that originates from a 'know yourself' position of understanding critical assets and using this understanding to be able to discover potential threats that are context sensitive to the organization. It also emphasizes that organizations possess a detection capability that understands profile of normal activity within an organization so that it can appropriately target external detection sources. Lastly, to enhance corporate knowledge about CTI, the OCTI model emphasizes an organizational learning component, and a component that emphasizes organizational learning through the sharing of CTI information with others in their competitive space.

The section below illustrates the Threat Response Capability, second major component of the OCTI model.

Threat Response Capability

A Threat Response Capability represents an organization's response capability to effectively control threats, and interact with the threat environment, either passively or actively. This is accomplished in three ways: through adaptation – an organization's ability to adapt to external threats, and external threat

environments. Through shaping – an organization's competency in re-shaping internal assets based on information they have received through Threat Analysis. And through selection – an organization's efficacy in making appropriate choices based on impact, urgency, and certainty.

Threats pose different levels of familiarity to an organization: on one end, newly-arriving, little known, and unfamiliar threats, and, on the other end, familiar, routine, or recurring type of threats. Virtually, all threats fall somewhere on the continuum between the two types as the majority of new threats are not necessarily created in vacuum. Little known and unfamiliar types of threats demands an organization's ability to craft sometimes creative solutions and countermeasures. An organization that have attained the highest level of adaptive capability in threat management (NIST, 2014) may respond better to such little-known threats as adversaries' TTPs continuously evolve. Meanwhile, the familiar, routine, or recurring threat types demand an organization to facilitate automated information processing, integration, and response (Montesino et al., 2012; Securosis, 2015). Automation is a key success condition when attacks and intrusions have to be mitigated at machine speeds (Fonash and Schneck, 2015). And as organizations with a CTI program will end up with inundation of threat-related data, an organization can marshal the above three different approaches to fend off internal and external threats, and adequately respond to evolving threat environments.

Adaptation

Adaptation is defined as an organization's capacity to formulate both strategic and functional controls to adapt to internal and external threats and threat environments, whilst keeping the core structure or system environment of an organizational intact. Thus, responses are largely intended to reinforce an organization's traditional adaptation capability (Fonash & Schneck, 2015; Los et al., 2014), as threat-related information obtained in the Threat Analysis phase acts as crucial input. Adaptation can take the form of throttling or suspending certain types of system access, plugging holes to reduce system vulnerability, temporarily suspending certain systems features until threats have been mitigated, throttling traffic to externally facing systems such as websites or APIs, or audit implementing controls intended to counter threats or offset attack vectors at the functional level reflect the "adaptation spirit" (Ransbotham & Mitra, 2009). The external threat environment and its threat forces are largely beyond an organization's control and, thus, an organization should have to capacity to actively adapt.

Shaping

Shaping represents an organization's competence to reshape the internal environment of an organization or a system that is conductive to threats by electing barriers through its structural or architectural changes. This mode of response is intended for shifting from "as is" environment into "to be" environment to offset threats (Vaughn, 1996). A shaping solution may have features of counterintelligence such as threat deception, neutralization, and/or deterrence through 'responsive' and/or an awareness/learning-propelled integrated risk management process (NIST, 2014). Moreover, shaping can also entail reengineering business processes, reforming security through insider policies, or other augmented security management (e.g., information flow control between trusted business partners) (Vaughn, 1996). In growing the OCTI capability to shape an organization's CTI response, an organization must be able to constantly and continuously transform its structure and security posture to create new environments more resistant to threats in the long run. From that perspective, shaping is not solely technical, but strategic, difficult, and may consume significant amounts of resources to devise and implement (as opposed to Adaptation), but stands to benefit organizations with longer-term resiliency.

Selection

'Selection' is an organization's competence to make adequate choices as to how it balances adaptation and shaping strategic and functional (operational and tactical) countermeasures in light of CTI and its expected impact, urgency, and certainty. In other words, Adaptation represents a shorter-term solution, which is effective in offsetting short-lived threats more quickly, and thus less costly to implement than those of shaping. In contrast, shaping is costlier to plan and implement, but carries the potential for greater longterm resiliency. Thus, 'selection' entails the appropriate balancing of Adaptation and Shaping,

the balancing of short term fixes with longer-term strategic CTI measures, so as to be able to respond quickly whilst being able to withstand prolonged threats such as Advanced Persistent Threats, or APTs (Hutchins et al., 2011). Useful to Selection are classification mechanisms for common threat domains such as the Common Attack Pattern Enumeration and Classification (CAPEC). However, the 'answer' as to how to respond depends on many factors. Depending on the type of CTI, a short-term control may be enough to neutralize threat potential, whereas, in other situations, a broader strategy may need to be implemented in order to implement comprehensive adaption and shaping measures. Without question, the choice being one with considerable organizational implications relating to return on investment (ROI) and long-term CTI success.

Conclusion

The age of hyper-connectivity has arrived and there is no shortage of alarming stories on severe security breaches these days. In this wake, it is observed that much of the information security paradigm has been fixated on the implicit assumption that mastering the 'know yourself' paradigm is key for success. There, however, has to be a balance in both knowing yourself and knowing your enemies. In cyberspace, knowing your enemies amounts to understanding threats, including the adversaries who facilitate threats, and thus, it is paramount in cybersecurity to understand and engage with the CTI battlefield. Organizations have traditionally 'played defense' against these invisible aggressors, and the process of OCTI stands to shift that tradition. This paper, therefore, takes the position that a CTI initiative is one that strengthens situational awareness, and facilitates organizations taking a more offensive position in the cybersecurity battlespace. OCTI represents a model that is actionable for decision makers, deriving from a 'know yourself' position in an effort to better 'know your enemies' in new ways. Thus, this research proposes a prescriptive capability model for an organization in undertaking CTI efforts to elucidate an organization's principal threat elements and their relationships.

References

Archer, D. W., & Wick, A. (2013). Peer-to-Peer Enclaves for Improving Network Defence. Technology Innovation Management Review, 3(7).

Argote, L., & Miron-Spektor, E. (2011). Organizational learning: From experience to knowledge. Organization science, 22(5), 1123-1137.

Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. IT professional, 12(1), 24-31.

Barnum, S. (2012). Standardizing cyber TRI information with the Structured Threat Information eXpression (STIX™). MITRE Corporation, 11.

Bhatt, S., Manadhata, P., & Zomlot, L. (2014). The operational role of security information and event management systems. IEEE Security & Privacy, 12(5), 35-41.

Bianco, D. (2013). The pyramid of pain. Retrieved, 01/23/2017, Retrieved from http://detectrespond.blogspot.com/2013/03/the-pyramid-of-pain.html.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS quarterly, 39(4), 837-864.

Bou-Harb, E., Debbabi, M., & Assi, C. (2014). Behavioral analytics for inferring large-scale orchestrated probing events.2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 506-511.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

Caglayan, A., Toothaker, M., Drapeau, D., Burke, D., & Eaton, G. (2012). Behavioral analysis of botnets for TI. Information Systems and E-Business Management, 10(4), 491-519.

Carcary, M., Doherty, E., & Thornley, C. (2015). Business Innovation and Differentiation: Maturing the IT Capability. IT Professional, (2), 46-53.

Chen, H. M., Kazman, R., Monarch, I., & Wang, P. (2016, May). Predicting and fixing vulnerabilities before they occur: a big data approach. In Proceedings of the 2nd International Workshop on BIG Data Software Engineering (pp. 72-75). ACM.

Chen, Y., Wang, Y., Nevo, S., Jin, J., Wang, L., & Chow, W. S. (2014). IT capability and organizational performance: the roles of business process agility and environmental factors. European Journal of Information Systems, 23(3), 326-342.

Chismon, D. & Ruks, M. (2015) TI: Collecting, Analysing, Evaluating, MWR Inforsecurity, https://www.cpni.gov.uk/Documents/Publications/2015/23-March 2015MWR_Threat_Intelligence_whitepaper-2015.pdf

Cole, E. (2014) Insider Threats in Law Enforcement. The SANS Institute.

Costa, D. L., Albrethsen, M. J., Collins, M. L., Perl, S. J., Silowash, G. J., & Spooner, D. L. (2016). An Insider Threat Indicator Ontology. Software Engineering Institute, Carnegie Mellon University.

Couch, J. (2015). The Need for a Threat Intelligence Maturity Model http://www.isightpartners.com/2015/07/the-need-for-a-threat-intelligence-maturity-model-pt-1/ (access on 4/22/2016)

Coyne, J., Neal, S., & Bell, P. (2014). Reframing intelligence: challenging the Cold War intelligence doctrine in the information age. International Journal of Business & Commerce, 3(5), 53-68.

Curley, M. & Kenneally, J. (2012) Executive Overview: IT Capability Maturity Framework, Innovation Value Institute.

Davis, P. K. (2014). Toward Theory for Dissuasion (or Deterrence) by Denial. http://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1027/RAND_WR1027.pdf (retrieved on 11/12/2016)

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, 20(1), 79-98.

Dhillon, G. (2015). What to do Before and After a CyberSecurity Breach. American University.

EY (2014). Achieving resilience in the cyber ecosystem, http://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EYInsights_on_GRC_Cyber_ecosystem.pdf (retrieved on 12/11/2015)

Filshtinskiy, S. (2013) Choosing controls to protect against targeted attacks: Application of the analytical TI, IET Conference Publications, v 2013, n 620 CP, 2013, 8th IET International System Safety Conference Incorporating the Cyber Security Conference

Fink, L. (2011). How do IT capabilities create strategic value? Toward greater integration of insights from reductionistic and holistic approaches. European Journal of Information Systems, 20(1), 16-33.

Fonash, P., & Schneck, P. (2015). Cybersecurity: From months to milliseconds. Computer, 48(1), 42-50.

Fransen, F., Smulders, A., & Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. e & i Elektrotechnik und Informationstechnik, 132(2), 106112.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. Information Systems Research, 16(2), 186-208.

Ghernouti-Hélie, S. (2010). A national strategy for an effective cybersecurity approach and culture. In Availability, Reliability, and Security, 2010. ARES'10 International Conference on (pp. 370-373). IEEE.

Giles, L. (1910). trans. Sun Tzu on the Art of War.

Hardy, G. M. (2012). Beyond Continuous Monitoring: Threat Modeling for Real-Time Response. The SANS Institute.

Heckman, K., Stech, F., Schmoker, B., & Thomas, R. (2015). Denial and deception in cyber defense. Computer, 48(4), 36-44.

Holland, R. (2013). Five Steps to Build an Effective TRI Capability. Forrester Research, http://www.coresecurity.com/system/files/attachments/2013/04/RickHollandFiveStepstoBuild.pdf

Honeycutt, D. (2016). Re: Intel comments in response to NIST's Solicitation for Comments on 'Views on the Framework for Improving Critical Infrastructure Cybersecurity' http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160218_Intel.pdf (downloaded on 12/12/2016)

Hsu, C., Lee, J. N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. Information systems research, 23(3-part-2), 918-939.

Hubbard, D. W. (2009). The failure of risk management: Why it's broken and how to fix it. John Wiley & Sons.

Hubbard, D. W., & Seiersen, R. (2016). How to measure anything in cybersecurity risk. John Wiley & Sons.

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. Leading Issues in Information Warfare & Security Research, 1, 80.

Iasiello, E. (2014). Is cyber deterrence an illusory course of action? Journal of Strategic Security, 7(1), article 6, 54-67. Available at: http://scholarcommons.usf.edu/jss/vol7/iss1/6 (downloaded on 12/20/2015)

Irwin, S. (2014). Creating a Threat Profile for Your Organization, The SANS Institute

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS quarterly, 549-566.

Johnson, C., Badger, L., & Waltermire, D. (2014) Guide to Cyber Threat Information Sharing, NIST Special Publication 800-150.

Karjalainen, Mari and Siponen, Mikko (2011) "Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches," Journal of the Association for Information Systems, 12(8), 518-566.

Kim, G., Shin, B., & Kwon, O. (2012). Investigating the Value of Sociomaterialism in Conceptualizing IT Capability of a Firm. Journal of Management Information Systems, 29(3), 327-362.

Kime, B.P. (2016). Threat Intelligence: Planning and Direction, The SANS Institute

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. MIS Quarterly, 38(2), 451-471.

Lakbabi, A., Orhanou, G., & El Hajji, S. (2012). Network access control technology—proposition to contain new security challenges. International Journal of Communications, Network and System Sciences, 5(8), 505-512.

Lee, J. K. (2015). Guest Editorial: Research Framework for AIS Grand Vision of the Bright ICT Initiative. Management Information Systems Quarterly, 39(2), iii-xii.

Lichtman, D., & Posner, E. (2006). Holding internet service providers accountable. Supreme Court Economic Review, 221-259.

Locke, K., & Golden-Biddle, K. (1997). Constructing opportunities for contribution: Structuring intertextual coherence and "problematizing" in organizational studies. Academy of Management journal, 40(5), 1023-1062.

Los, R., Robinson, J., Clark, J., Brooks, R. & Brown, W. (2014). TI, Accuvant,, http://files.accuvant.com/web/file/d96f8c4996ee4571999bcf513126399c/Threat%20Intelligence_Solution%20Primer.pdf

McBride, M., Carter, L., & Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. Prepared by RTI International–Institute for Homeland Security Solutions under contract 3-312-0212782, 1(1), 1-40.

Miles, C., Lakhotia, A., LeDoux, C., Newsom, A., & Notani, V. (2014, August). VirusBattle: State-of-the-art malware analysis for better cyber TI. In Resilient Control Systems (ISRCS), 2014 7th International Symposium on (pp. 1-6). IEEE.

Miron, W., & Muita, K. (2014). Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. Technology Innovation Management Review, 4(10).

Montesino, R., Fenz, S., & Baluja, W. (2012). SIEM-based framework for security controls automation. Information Management & Computer Security,20(4), 248-263.

Muckin, M. & Fitch, S. (2015). A Threat-Driven Approach to Cyber Security, Lockheed Martin Corporation.

http://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/ThreatDriven%20Approach%20whitepaper.pdf (downloaded on 12/12/2016).

National Institute of Standards and Technology (NIST) (2013). Security and privacy controls for federal information systems and organizations. NIST Special Publication, 800-53, Revision 4,

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (downloaded on 12/12/2016).

National Institute of Standards and Technology (NIST) (2014). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0). http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (downloaded on 12/12/2016).

National Institute of Standards and Technology (NIST) (2016). Cybersecurity Framework Feedback: What We Heard and Next Steps. https://www.nist.gov/sites/default/files/workshop-summary2016.pdf (downloaded on 12/12/2016).

National Security Agency (NSA). (2018) Defense in depth: a practical strategy for achieving information assurance in today's highly networked environments. https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf (accessed January 15, 2018).

NTT Group (2014). Global TRI Report, https://www.dimensiondata.com/Global/Downloadable%20Documents/2014%20NTT%20Group%20Global%20Threat%20Intelligence%20Report.pdf (retrieved on 12/11/2015)

Pfleeger, S. L., & Rue, R. (2008). Cybersecurity economic issues: Clearing the path to good practice. Software, IEEE, 25(1), 35-42.

Patrick, R. (2006) Effective Operational Security Metrics. Information Systems Security. 15(3), 10

Poputa-Clean, P. (2015). Automated Defense Using TRI to Augment Security. The SANS Institute, https://www.sans.org/reading-room/whitepapers/threats/automated-defense-threat-intelligenceaugment-35692 (downloaded on 12/11/2015).

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. Mis Quarterly, 757-778.

Prunckun, H. (2014). Extending the theoretical structure of intelligence to counterintelligence. Salus Journal, 2(2), 31-49.

Ramachandran, Sriraman; Rao, Chino; Goles, Tim; and Dhillon, Gurpreet (2013) "Variations in Information Security Cultures across Professions: A Qualitative Study," Communications of the Association for Information Systems, 33(11), 1-40.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. Information Systems Research, 20(1), 121-139.

Ring, T. (2014) TI: Why people don't share, Computer Fraud and Security, n 3, p 5-9.

Rowe, B., Wood, D., Reeves, D., & Braun, F. (2011). Economic analysis of ISP provided cyber security solutions. Institute for Homeland Security Solutions, 36.

Sager, T. (2014). Killing Advanced Threats in Their Tracks: An Intelligent Approach to Attack Prevention. The SANS Institute.

Santos Jr, E., Nguyen, H., Yu, F., Kim, K., Li, D., Wilkinson, J. T. & Jacob, R. (2008). December). Intentdriven insider threat detection in intelligence analyses. In Proceedings of the 2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology-Volume 02(pp. 345349). IEEE Computer Society.

Securosis (2015). Applied Threat Intelligence. https://securosis.com/assets/library/reports/Securosis_AppliedThreatIntelligence-FINAL.pdf (downloaded on 12/11/2015)

Shackleford, D. (2015). Who's Using Cyberthreat Intelligence and How? The SANS Institute.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 487-502.

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security" De Jure" Standard in a Government Organization. MIS quarterly, 463-486.

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS quarterly, 503-522.

Sternberg, R. J. (1999). The Theory of Successful Intelligence. Review of General Psychology, 3(4), 292316.

Sternberg, R. J. (2003). A Broad View of Intelligence: The Theory of Successful Intelligence. Consulting Psychology Journal: Practice and Research. 55(3), 139-154.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS quarterly, 441-469.

Susskind, N. G. (2014). Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know. NYUJL & Bus., 11(1), 573.

Thonnard, O., & Dacier, M. (2008). Actionable knowledge discovery for threats intelligence support using a multi-dimensional data mining methodology. 2008 IEEE International Conference on Data Mining Workshops, 154-163.

Townsend, T., Ludwick, M., McAllister, J., Mellinger, A. O., & Sereno, K. A. (2013). SEI Innovation Center Report: Cyber Intelligence Tradecraft Project: Summary of Key Findings. Carnegie-Mellon University, Pittsburgh PA, Software Engineering Institute

Vaughn, R. B. (1996). A Practical Approach to Sufficient Infosec. In National Information System Security Conference (pp. 1-11).

Vanderpol, M., Hellbusch, S. A., & Hale, R. W. (2015). U.S. Patent No. 9,065,799. Washington, DC: U.S. Patent and Trademark Office.

Vratonjic, N., Manshaei, M. H., Raya, M., & Hubaux, J. P. (2010, November). ISPs and ad networks against botnet ad fraud. In International Conference on Decision and Game Theory for Security (pp. 149-167). Springer Berlin Heidelberg.

Webb, J., Maynard, S., Ahmad, A., & Shanks, G. (2014). Information Security Risk Management: An Intelligence-Driven Approach. Australasian Journal of Information Systems, 18(3).

Wang, J., Chaudhury, A., & Rao, H. R. (2008). Research Note-A Value-at-Risk Approach to Information Security Investment. Information Systems Research, 19(1), 106-120.

World Economic Forum (2015). Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats, available at

www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf (downloaded on 12/11/2015)

Yang, N. (2014). The impact of the organizational innovation on strategic change: Cognitive and learning perspectives. In Management Science & Engineering (ICMSE), 2014 International Conference on (pp. 408-416). IEEE.

Zafar, H, and Clark, J.G. (2009) "Current State of Information Security Research In IS," Communications of the Association for Information Systems: 24(34).

Zhang, M., Sarker, S., & Sarker, S. (2013). Drivers and export performance impacts of IT capability in 'born-global' firms: a cross-national study. Information Systems Journal, 23(5), 419-443.

Zhuo, Y., & Solak, S. (2015). Cybersecurity investment optimization with risk: Insights for resource allocation. In Industrial Engineering and Operations Management (IEOM), 2015 International Conference on (pp. 1-13). IEEE.