



SUPPLY CHAIN AND LOGISTICS MANAGEMENT AND AN OPEN DOOR POLICY CONCERNING CYBER SECURITY INTRODUCTION

 **Darrell Norman Burrell**¹⁺

Nimisha Bhargava²


Orna Bradley-

Swanson³

Maurice Harmon⁴

Jorja Wright⁵

Delores Springs⁶

 **Maurice Dawson**⁷

¹Florida Institute of Technology, USA.

²Email: arrell.burrell@yahoo.com Tel: (804)765-4665

³National Institute of Industrial Engineering, India.

⁴Email: amiabile.nimisha@gmail.com

⁵Walden University, USA.

⁶University of Phoenix, USA.

⁷University of Charleston, WV, USA.

⁸Regent University, USA.

⁹Illinois Institute of Technology, USA.



(+ Corresponding author)

ABSTRACT

Article History

Received: 8 October 2019

Revised: 15 November 2019

Accepted: 17 December 2019

Published: 24 January 2020

Keywords

Logistics management

Cybersecurity

Human factors cybersecurity

Whistleblowing.

The need for integrity and reliability in the supply chain and logistics management operations has a well-established array of theoretical frameworks that guide organizations and managers in the field. However, what is missing is a comprehensive, established framework for logistics and supply chain cybersecurity. The emerging area of cyber-supply chain security continues to lack suitable models to help secure critical data and systems. In all industries and fields today, cybersecurity is no longer just an information technology issue. It is a business sustainability and business strategy issue. The human factors in the cyber-supply chain operations represent the actions or events when human error results in a successful hack or data breach. Today, protecting logistics and supply chain organizations from cyber and data security risks is no longer just an information technology employee function. Every organizational employee has a responsibility in the data protection process. Progressive organizations are ones that can create methods, policies, and approaches that encourage employees to play an active role in the information and cybersecurity process. This paper explores innovative approaches around open-door systems as a proactive data security and cybersecurity risk reduction organizational strategy. This research provides cyber-supply chain practitioners and scholars an array of concepts to help them understand and describe the dynamics of cyber-supply chain and logistics management data security vulnerabilities and opportunities for process improvements.

Contribution/Originality: This study contributes to the existing literature by exploring innovative approaches around open-door systems as a proactive risk reduction approach.

1. INTRODUCTION

In the U.S. alone, cybercrimes have had a detrimental impact on the country's economy; costing approximately 445 billion annually (Simon and Omar, 2020). Supply chain managers' heavy reliance on information technology

(IT) to improve organizational systems, infrastructure, competitive advantage, and growth have inadvertently increased their organizations' cybersecurity vulnerabilities (Lee and Rha, 2016; Windelberg, 2016). According to Alamoudi and Alamoudi (2016) "no software or technology is without risks or issues" (p.59). Urciuoli and Hintsa (2017) asserted that cyber risk in a supply chain is a significant and emerging threat to supply chain companies' competitive advantage. Especially since, cyber-attacks have gone up 300% in the past three years (Martin *et al.*, 2017).

As stated by Simon and Omar (2020) more than 60% of cybersecurity breaches on supply chains are through suppliers or third-party logistics. Companies such as Target, Home Depot, Fiat Chrysler, Costco, and Sam's Club were all cyber-attacked through third-party suppliers or service providers (Simon and Omar, 2020). Through third party suppliers, cyber attackers used computer viruses, hacking, malware, and ransomware to facilitate criminal activities on IT hardware and software of organization with the supply chain to gain access to targeted business (Dhillon and Backhouse, 1996; Urciuoli and Hintsa, 2017). This security vulnerability is inherent when most supply chains consist of multiple suppliers, with suppliers having their own suppliers (Windelberg, 2016); each of them using various systems with different levels of IT security to access data from "purchase orders, shipping instructions, bills of materials, warehouse packing list (Urciuoli and Hintsa, 2017).

1.1. The Object of Research

The focus of this research is an exploration of theories and concepts in information security, data security, cybersecurity, organizational behavior, and supply chain management research.

1.2. The Goal of Research

The goal of this research is to influence the practitioner world of management practice and business process improvement that could serve tools to improve employee engagement approaches for supply chain and logistics organizations in the areas of data security, cybersecurity, and information security,

2. RESEARCH METHODS

The research approach is the engagement of content analysis in the literature and the argumentative review of knowledge theories in management science, whistleblowing, information security, cybersecurity, data security, supply chain management, and organizational behavior to develop tools to improve management practice.

2.1. Overview

Supply chain managers and suppliers share a large amount of data to support communication and collaborative efforts as well as build trust in the supply chain management process (Urciuoli and Hintsa, 2017). According to Boiko *et al.* (2019) "the chains of manufacturers, suppliers, contractors, transport and trading companies are intertwined in the most intimate way and are already real online networks" (p. 67). Supply manager leverage IT to support Radio Frequency Identification (RFID), Enterprise Resource Planning (ERP) and Electronic Data Interchange (EDI) to increase visibility along the supply chain (Li and Chandra, 2007; Caridi *et al.*, 2014). The need to quickly respond to customer requirements, and to manage partnering networks can increase cybersecurity vulnerabilities and have significant and cascading negative impacts on a business. For example, Target 2013 breach through a service provider led to the compromise of more than 110 million customer personal data; and costing the company a total of over \$200 million in financial loss (Simon and Omar, 2020). In addition to the financial impact, cyber-attacks through third parties can affect supplier-buyer relationships. Cyber-related risks are disruptive and can a negative impact on an organization's competitive advantage (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). Because information security risks are so significant, supply managers must understand security vulnerabilities to

develop appropriate ethical security strategies to promote, protect, and prevent harm to customers, partners, and all stakeholder.

Organizations respond to information security attacks using defensive measures and risk minimization methods (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). Information security incident management is a set of defensive measures for identifying technology, processes, and people responsible for attacks and infiltrations against assets to violate the confidentiality, integrity, or availability of the asset and using that information to diagnose, contain, and recover from incidents (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). The management of information security incidents helps organizations to minimize the damages caused by attackers. Information security incident management is a unique marriage of the elements of offensive information security and defense strategy (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019).

The extremely high and growing volume of information security incidents must be addressed by scholar-practitioners in order to discover the nature of the phenomenon and stem the tide of this increasing dilemma (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). There is a lack of empirical research demonstrating holistic organizational and managerial behavioral responses to information security exposures and innovative risk management approaches (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). Because of the fragmented nature of the literature around organizational behavioral and managerial behavioral approaches to data, cyber, and information security, there is value exploring information and data security from these approaches (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). This research will add to the body of knowledge regarding elements of information security and data security through the exploration of gaps of this topic around supply chain and logistics management.

Due to the lack of significant academic research on data security and the fast changing dynamics in the field, information security and data security seminal conceptual and theoretical literature in the field is still emerging and being developed (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). Information and data security are more dynamic, emerging, and chaotic fields than the fields of computer science and information technology, which are based on concepts and theories that are long established (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). New hazards, dangers, and susceptibilities are unearthed each year in the field and the world of practice (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). These emerging dangers is often reported through industry reports and corporate research rather than academic research (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019).

2.2. Data Security and Information Security Concepts

There are a variety of ideas and concepts that apply to data, cyber, and information security in the supply chain and logistics management process. Organizational assets are often the target of attackers attempting to steal data or information (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). An asset can be a database, employee information, organizational intellectual property, technology system or application, or any other form of valuable digital information (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). All of these assets can be targeted and should be protected from attack as part of a comprehensive organizational security strategy (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). For supply chain and logistics organizations assets could be client lists, customer payment information, or even business operation protocols.

Defending information security covers a wide area of preventive and reactive tasks that contribute to the security of information (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). Defensive information security consists of the preventive management of risk as well as the reactive management of information security incidents (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). These defensive categorizations of processes and procedures each cover a wide variety of tasks directly related to the security of information in the logistics management and supply chain management process.

Information and data security are the identification of technology assets and targets, the processes of defending or attacking those technology assets and targets, and the social constructs influencing attackers and defenders

(Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). These elements inform all aspects of information security as a common ontological framework in the supply chain and logistics management operational process.

Information security incident in an event that adversely affects technology systems or services, must relate to the elements of information security, including the identification of assets, processes for attack and defense, and human attackers and defenders (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019).

Information security incident management is identifying technology, processes, and people responsible for attacks and infiltrations against assets to violate the confidentiality, integrity, or availability of the asset and using that information to diagnose, contain, and recover from incidents (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019).

Risk management covers the implementation of information security in practice (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). Risk management is how information security is performed in modern organizations through the analysis and evaluation of vulnerabilities against threats to determine risk and the mitigation of that risk based on organizational priorities (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019).

A significant number of data security and cybersecurity threats come from human nature and a lack of organizational due diligence (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019)). Human factor as a security weakness in information security has gained increased attention, especially when security technologies have failed to prevent cyber breaches (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). Industry professionals feel that people and their actions or inaction represent one the most critical vulnerabilities in the management of information security risks (Burkhead, 2014; Okonofua, 2018; Djatsa, 2019). Any process that can diminish the human risk and can empower employees to constructively contribute in risk mitigation is an avenue in need of significant exploration in supply chain and logistics operations management. Creating processes where employees can play an active role in addressing organizational security weaknesses is an important aspect in making organizational data more secure in supply chain and logistics organizations.

2.3. Supply Chain Cybersecurity Ethical Consideration

Fantazy and Tipu (2019) stated the supply chain has a culture of competitiveness which influences innovation, entrepreneurship, and organizational learning. Correspondingly, Madani and Wajeetongratana (2019) found a supply chain culture of competitiveness improved productivity and increased employee performance in an organization. However, a supply chain with many employees focused on innovating to gain a competitive advantage, increases an organization's cyber risk and potential for disruption in information technology (IT) system operations (Boyson, 2014). Colicchia *et al.* (2019) found that employees are increasingly being used as tool for malicious attacks. This assertion supports (Boiko *et al.*, 2019) where the researchers found that end-suppliers, sub-contractors, third-party personnel underestimate the risk cyber vulnerabilities associated with loopholes in their corporate network, cloud, and end-device infrastructure; as a result, some personnel will connect various Internet of Things (IoT) devices to their organization's dynamic network infrastructure. Security managers struggle to identify cyber warnings from connected IoT devices and consequently, the responsible employee in the case of an attack on IoT devices (Boiko *et al.*, 2019). Colicchia *et al.* (2019) stated that cybersecurity non-compliant behaviors are deliberate choices that could lead to underestimating the consequences of actions on the supply chain, with oblivious victims of a cyber-attack.

When information security breaches occur, supply chain managers must be open and honest with those impacted and at risk. The U.S. Securities and Exchange Commission (2018) outlined that companies should have controls and procedures in place to properly evaluate cyber incidents and disclose material information to customers. Often organizations do not openly disclose the extent and nature of data thefts and breaches, and often it is whistle-blowing that leads to the public finding out the severity of the attack (Bhargava *et al.*, 2018). These data breaches and failures to disclose their severity require the need for cultures around the ethical and organizational importance of whistleblowing when there are cybersecurity breaches (Bhargava *et al.*, 2018).

2.4. The Whistle-Blower

A whistle-blower is one who provides information on a person or organization participating in an unlawful activity (Bazzetta, 2015). Similarly, Lee (2005) and Stewart (1996) described a whistle-blower as an individual who reveals necessary acts of fraud, corruptions, abuse, waste, or misuse of power or authority in breach of the country's laws or regulations in either the public or private sector. Miceli and Near (1992) defined whistle-blowing as the disclosure by current or former members of an organization of immoral, unethical, illegitimate, or illegal activities related to an organization or its employees. Other researchers described whistle-blowing as an ethical issue of great significance in protecting all stakeholders against activities that may adversely impact economic, environmental, financial, and public safety, whether locally or globally (Courtemanche, 1988; Weiss, 2006; Hoffman and McNulty, 2010).

2.5. Whistle-Blowing and Whistle-Blowing Traits

Whistle-blowing is among the conceivable possibilities an employee can choose to relay illicit information. As given by Bazzetta (2015) whistle-blowing is the revelation by organizations' members, past or present, of illegal, immoral or prohibited practices under the influence of their employers, to individuals/organizations that could have the ability to influence action. While whistle-blowing is a complex process involving personal and organizational cultural factors; it is the primary instrument for encouraging individual and organizational accountability (Wilde, 2013). Research on whistle-blowing is essential because unethical behavior is a continuing problem in a variety of organizations (Bhargava *et al.*, 2018). Serious consequences can result from whistle-blowing, both for an organization and for the individual whistle-blower, who may suffer intimidation, termination, marginalization, and isolation as forms of retaliation (Wilde, 2013). Both the positive and negative aspects of whistle-blowing deserve critical attention (Bhargava *et al.*, 2018).

An additional viewpoint addressed the complexities around ethics, openness, and honesty around choosing to whistle-blow are not when issues arise (Bhargava *et al.*, 2018). Employees often face quandaries amid being steadfast to the organization while maintaining strong values towards righteousness and justice (Waytz *et al.*, 2013). The result of this conflict is often an emotional reasoning struggle for employees that are firmly committed organizational citizens that cannot stay quiet when wrong, when questionable things are observed, even if speaking out about the wrong, could tarnish the perception and reputation of that organization (Bhargava *et al.*, 2018).

Vadera *et al.* (2009) stated the elements that influenced honesty and speaking up in an organization include:

- Leadership and organizational governance.
- Perceived backing and support.
- Organizational justice.
- Organizational climate and culture.
- Organizational type and structure.
- Risk of reprisal.

With the increase in cybercrimes and identity thefts, it is crucial for both supply chain managers and information security managers to understand the importance of embracing ethical cultures, moral reasoning, and ethical decision making. Urciuoli and Hints (2017) asserted that most supply chain managers were unaware of their supply chain exposure to cyberattack because they lacked visibility across the entire supply chain. This assertion supports the need for whistleblowing. If there is a breach that impacts costumers' information; the ethical approach is to notify personnel at risks immediately so they can employ appropriate mitigating actions without delay. Equally as important, supply managers must promote an organizational culture of IT Safety; encouraging everyone in the company actively supports information security efforts (Bhargava *et al.*, 2018). The use of information technology solutions that support supply chain management and operations to include supply chain visibility has grown exponentially in the past few decades (Simchi-Levi *et al.*, 2008). Because business have the

responsibility of adequately securing personal information like credit card information and social security data; it is critical for them to promote ethical decision making at all levels and create avenues for employees to come forward when there are concerns around ethics and integrity.

The figure below represents a flowchart model proposed by Bhargava *et al.* (2018) which represents the six levels of ethical, moral, and legal decision making when emotions are involved around whistle-blowing.

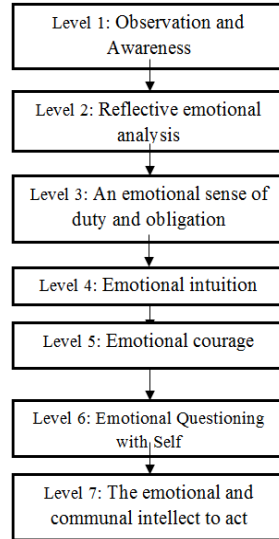


Figure-1. Emotional acumen model for ethical, moral, and legal decision making.
 Source: Bhargava *et al.* (2018).

Table-1. Burrell and Bhargava Emotional acumen model for ethical, moral, and legal decision making Burrell and Bhargava emotional acumen model for ethical, moral, and legal decision making.

| | |
|---------|---|
| Level 1 | Observation and Awareness – At this stage, there is a discovery, observation, and a witness of an ethical, moral, or legal issue of concern. |
| Level 2 | Reflective emotional analysis – At this stage, there is a level of significant disquiet that leads to a deeply reflective and critical emotional examination about the issue of concern and how serious it is or has the potential to be. At this stage, an individual must try his/her best to gather the facts and be as neutral as possible while describing or analyzing those facts. One should not be inclined towards distorting the facts or information for his/her personal benefits. |
| Level 3 | An emotional sense of duty and obligation – At this stage, there is either an emotional inability to remain a bystander about the issue and not do anything about it, or there is personal emotional onus and responsibility to act. |
| Level 4 | Emotional intuition – This stage is about intuitions or conscience. When our emotions are cultivated by compassion, then they at times highlight what our cognizant and coherent mind has overlooked. Our emotions are one mode to check or to see whether one is rationalizing. |
| Level 5 | Emotional courage – At this stage, there is a deep exploration of the range of emotions that could include fear of retaliation and apprehension of the potential backlash, but there are still compelling overriding reasons to take action and do something. Here, a prediction about the future is made, which is relevant to the situation(s) at hand. Though an individual can never predict the future, yet certain things are more likely than others. |
| Level 6 | Emotional Questioning with Self – At this stage, an individual should always ask oneself before acting the following questions: a) Will I be able to live with myself if I made a particular choice? b) Will I feel better or worse about myself? c) Am I willing to let other people know about the situation or my decision to act? d) Will I feel guilty or ashamed of not taking any action sooner, or will I feel proud of my decision to act? e) Do I want everyone around me to act the way I did? |
| Level 7 | The emotional and communal intellect to act – At this stage, there is an understanding of how to manage the emotional perceptions and emotional consequences that are required to act and navigate the social interactions, politics, and fallout. |

Note: Burrell and Bhargava Emotional Acumen Model for Ethical, Moral, and Legal Decision Making Created by Dr. Darrell Norman Burrell and Dr. Nimisha Bhargava.

3. CONCLUSIONS AND RESULTS

Information Security Management is a set of policies, standards, and procedures by which an organization protects its vital information assets, especially the ones that hold sensitive information, and close the gap in their security systems and processes through risk management (Gardiyawasam and Oleshchuk, 2016). An information security policy is the foundation of any information security management system as it defines the roles, responsibilities, and decision-making activities that tie information security in the daily business processes and procedures (Edwards, 2013). A corporate security policy typically defines the domain to be protected, access control to assets, and the number of resources that need to be committed based on the identified criticality of the protected assets. However, security policies are often at crossroads with costs and user experience, hence making it difficult for security professionals to maintain them. Management support is, therefore, critical to the successful implementation and execution of security policies; thus, the commitment of the executive tier of management is a requirement for fair resource allocation essential for policy implementation (Soomro *et al.*, 2016). In the past, much of the efforts on information security were focused on technical modalities and solutions to deal with security threats and attacks; however, these efforts have now shifted more towards the human factor, and on the need for the alignment of IT to business objectives. This assertion is consistent with Boyson (2014) where the researcher asserted that supply chain manager must deal with their employees' behavior to reduce cyber risks and disruption in IT system operations. As a result, the need to have systems that encourage employees at all levels to support the information security apparatus has never been more critical.

Symantec (2019) reported that supply chain attack using third-party suppliers increased by 78% between 2017 and 2018. Data breaches are impactful to the affected customers as well as the businesses involved. Researchers' opinions on the fundamental cause of security breaches are diverse and include that most data breaches are a result of insufficient security of critical or sensitive data, malicious employee theft, and intrusion attempts (Holtfreter and Harrington, 2015). Many data breaches are caused by inadvertent disclosure of information; however, some research work has analyzed very large breaches. One such study analyzed 2633 data breaches that cost U.S. organizations over 500 million lost individual records between 2005 and 2011 (McLeod and Dolezel, 2018). The conclusion from the resultant investigations is that human factors and the institution of security policies were significantly related to an increase in data breaches, thereby fueling the call for organizations to invest more in security and tight integration of processes and workflow with security (McLeod and Dolezel, 2018). Results from McLeod and Dolezel (2018) study on factors associated with data breaches show that human actions, behavior, organizational culture, and personal motivation are leading causes of security breaches. Employees of companies within the supply chain are often given unmonitored access to confidential information so they can effectively execute their job. This lack of oversight can ultimately pose information security governance concerns.

Some leaders are more comfortable to authorize the purchase of automated solutions instead of investing in the effort to change the corporate culture (McLeod and Dolezel, 2018). This attitude often results in an environment with detached, challenging solutions that produce inherent security holes (McLeod and Dolezel, 2018). What does an organization that supports the whistle-blowing/open door process/policy around information security look like? Below is an information security framework that is critical to creating an organizational culture where all employees can assist in minimizing and addressing information security risks.

A content analysis review of the literature yielded some solid insights and a usable framework. The Burrell Whistle Blowing/Open Door Information Security Model Framework (2020) framework (Table 2) is built off the U.S. Department of Homeland Security that was focused on terrorism but also applies to the supply chain management data security process that tells all stakeholders, *if you see something, say something*.

Table-2. Burrell whistle blowing/open door information security model framework (2020).

| | |
|-----------|---|
| | <ul style="list-style-type: none"> • Burrell Whistle Blowing/Open Door Information Security Model Framework (2020) |
| Element 1 | <ul style="list-style-type: none"> • A clear definition of what constitutes a cybersecurity whistle-blower. An example could be: An information security "whistle-blower" is an individual who reports information he/she reasonably believes pieces of evidence: A violation of any law, rule, or regulation around information security. • Gross mismanagement which would include a substantial risk of significant adverse impact on a mission around the protection and security of personally identifiable information (PII). • Abuse of authority: an arbitrary decision for personal gain and to injure others concerning information security. • A substantial and specific danger to public health or safety concerning information security. • A "reasonable belief" generally means that a disinterested observer with knowledge of the essential facts known to and readily ascertainable by the employee or applicant can reasonably conclude that the actions of the agency official evidenced such violation, mismanagement, waste, abuse, or danger. This standard excludes rumors, speculation, and nonspecific allegations. |
| Element 2 | <p>A clear and formal process for information security whistle-blowers to disclose observable risks, errors, and possible wrongdoing including:</p> <ul style="list-style-type: none"> • A managerial open door formal process that allows employees at all levels to discuss any cybersecurity or information security work-related issue or concern with any organizational supervisor or manager beyond informal discussions with his or her immediate supervisor. • An anonymous reporting hotline and an anonymous reporting process. • Strict prohibitions and employee protections against retaliation for protected disclosures and remedies if they have been retaliated against for making protected disclosures. This would prohibit threats and adverse personnel actions against an employee because he or she disclosed wrongdoing. Adverse personnel actions include poor performance reviews, demotion, suspension, or other forms of retaliation for filing an appeal, complaint, or grievance. |
| Element 3 | <p>Employee engagement actions focused on creating an organizational culture that is respectful and encourages all employees to raise concerns and differing views promptly and without fear of reprisal. The free and open exchange of views or ideas, conducted in a non-threatening environment, provides a forum where concerns and alternative views can be considered and addressed in an efficient and timely manner around information security management.</p> |
| Element 4 | <p>Training and awareness programs for all employees.</p> |
| Element 5 | <p>Staff ownership and employee resources that can manage the program and can fairly and properly investigate submissions and complaints.</p> |

While the supply chains remain customer-focused and managers continue share data across entire supply chain of partners, suppliers, manufacturers, and logistics providers for strategic advantage; it vital for those managers to consider security vulnerability implications (Mutek and Irwin, 2018). Li and Chandra (2007) asserted that even with assured information security, information warfare is uncertain and complex. However, Boiko *et al.* (2019) stated that supply managers must solve the complex problem of information security to include developing solution to secure data in supply chain management information systems. As cyber security risk increases through loopholes in third party suppliers' IT security; it is important that supply managers take an active role in safeguarding customer confidential information. Boiko *et al.* (2019) recommended that in the absence of real-time cyber security to ensure control, there is a need for real-time monitoring. As personnel monitor, they should also adopt the U.S. Department of Homeland Security mantra, if you see something, say something. Managers must promote an ethical organizational culture focused on confidentiality and information/data security to avoid causing harm or distress to customers. Whistleblowing is one of several strategies to promote ethical behavior. Future research may focus on other strategies to promote ethical behaviors to protect not only the supply managers' interests but the interests of the customers and end users (Mutek and Irwin, 2018).

Funding: This study received no specific financial support.

Competing Interests: The authors declare that they have no competing interests.

Acknowledgement: Both authors contributed equally to the conception and design of the study.

REFERENCES

- Alamoudi, Y. and W. Alamoudi, 2016. Cloud computing - the future of business. *Journal of Information Systems Technology and Planning*, 8(19): 41–60.
- Bazzetta, D.J., 2015. Whistle-blowers and post-conventional moral development: Toward identifying ethical & moral leadership (Order No. 3688375). Available from ABI/INFORM Collection. (1673895415).
- Bhargava, N., M.K. Madala and D.N. Burrell, 2018. Emotional acumen on the propensity of graduating technology students to whistle-blow about organizational cyber security breaches. *International Journal of Smart Education and Urban Society (IJSEUS)*, 9(4): 1-14. Available at: <https://doi.org/10.4018/ijseus.2018100101>.
- Boiko, A., V. Shendryk and O. Boiko, 2019. Information systems for supply chain management: Uncertainties, risks and cyber security. *Procedia Computer Science*, 149: 65-70. Available at: <https://doi.org/10.1016/j.procs.2019.01.108>.
- Boyson, S., 2014. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7): 342-353. Available at: <https://doi.org/10.1016/j.technovation.2014.02.001>.
- Burkhead, R.L., 2014. A phenomenological study of information security incidents experienced by information security professionals providing corporate information security incident management (Order No. 3682325). Available from ProQuest Dissertations & Theses Global.
- Caridi, M., A. Moretto, A. Perego and A. Tumino, 2014. The benefits of supply chain visibility: A value assessment model. *International Journal of Production Economics*, 151: 1-19.
- Colicchia, C., A. Creazza and D.A. Menachof, 2019. Managing cyber and information risks in supply chains: Insights from an exploratory analysis. *Supply Chain Management: An International Journal*, 24(2): 215-240. Available at: <https://doi.org/10.1108/scm-09-2017-0289>.
- Courtemanche, G., 1988. The ethics of whistle-blowing. *The Internal Auditor*, 45(1): 36- 41.
- Dhillon, G. and J. Backhouse, 1996. Risks in the use of information technology within organizations. *International Journal of Information Management*, 16(1): 65-74. Available at: [https://doi.org/10.1016/0268-4012\(95\)00062-3](https://doi.org/10.1016/0268-4012(95)00062-3).
- Djatsa, F., 2019. Examining the relationship between millennial professionals' perceptions of cybersecurity risks and users' online security behaviors (Order No. 22623854). Available from ProQuest Dissertations & Theses Global. (2308215337).
- Edwards, C.K., 2013. A framework for the governance of information security (doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global. (Order No. 3607548).
- Fantazy, K. and S. Tipu, 2019. Exploring the relationships of the culture of competitiveness and knowledge development to sustainable supply chain management and organizational performance. *Journal of Enterprise Information Management*, 32(6): 936-963. Available at: <https://doi.org/10.1108/jeim-06-2018-0129>.
- Gardiyawasam, P.H.S. and V.A. Oleshchuk, 2016. Privacy preserving mechanisms for enforcing security and privacy requirements in e-health solutions. *International Journal of Information Management*, 36(6): 1161-1173. Available at: <https://doi.org/10.1016/j.ijinfomgt.2016.07.006>.
- Hoffman, W. and R.E. McNulty, 2010. A business ethics theory of whistle-blowing: Responding to the \$1 trillion question. In M. Arszulowicz & W. Gasparski, (Eds.), *Defense of Proper Action: The whistle-blowing*. Piscataway, NJ: Transaction Publishers. pp: 45-60.
- Holtfreter, R.E. and A. Harrington, 2015. Data breach trends in the United States. *Journal of Financial Crime*, 22(2): 242-260. Available at: <https://doi.org/10.1108/jfc-09-2013-0055>.
- Lee, E., 2005. Whistleblowers: Heroes or villains. *Accountants Today*, August 2005: 14-18.

- Lee, S.M. and J.S. Rha, 2016. Ambidextrous supply chain as a dynamic capability: Building a resilient supply chain. *Management Decision*, 54(1): 2-23. Available at: <https://doi.org/10.1108/md-12-2014-0674>.
- Li, X. and C. Chandra, 2007. A knowledge integration framework for complex network management. *Industrial Management & Data Systems*, 107(8): 1089-1109. Available at: <https://doi.org/10.1108/02635570710822769>.
- Madani, M. and P. Wajeetongratana, 2019. The effects of culture and human resources management policies on supply chain management strategy. *Polish Journal of Management Studies*, 19(1): 235-248. Available at: <https://doi.org/10.17512/pjms.2019.19.1.18>.
- Martin, G., P. Martin, C. Hankin, A. Darzi and J. Kinross, 2017. Cybersecurity and healthcare: How safe are we? *British Medical Journal (Clinical research ed.)*, 358: j3179-j3179. Available at: <https://doi.org/10.1136/bmj.j3179>.
- McLeod, A. and D. Dolezel, 2018. Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, 108: 57-68. Available at: <https://doi.org/10.1016/j.dss.2018.02.007>.
- Miceli, M. and J.P. Near, 1992. *Blowing the whistle*. New York: Lexington Books.
- Mutek, M.W. and A.D. Irwin, 2018. Focus on supply chain risk management. *Contract Management*, 58(11): 26-37.
- Okonofua, H.I., 2018. The effects of information technology leadership and information security governance on information security risk management in usa organizations (Order No. 13426600). Available from ProQuest Dissertations & Theses Global. (2185921827).
- Simchi-Levi, D., P. Kaminsky and E. Simchi-Levi, 2008. *Designing and managing the supply chain concepts, strategies and cases*. 3rd Edn., New York: McGraw-Hill Book Company.
- Simon, J. and A. Omar, 2020. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, 282(1): 161-171. Available at: [10.1016/j.ejor.2019.09.017](https://doi.org/10.1016/j.ejor.2019.09.017).
- Soomro, Z.A., M.H. Shah and J. Ahmed, 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2): 215-225. Available at: <https://doi.org/10.1016/j.ijinfomgt.2015.11.009>.
- Stewart, D., 1996. *Organization ethics*. New York: McGraw-Hill Companies, Inc.
- Symantec, 2019. ISTR Internet Security Threat Report. Available from <https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf>.
- The U.S. Securities and Exchange Commission, 2018. SEC adopts statement and interpretive guidance on public company cybersecurity disclosures. Available from <https://www.sec.gov/news/press-release/2018-22>.
- Urciuoli, L. and J. Hintsas, 2017. Adapting supply chain management strategies to security—an analysis of existing gaps and recommendations for improvement. *International Journal of Logistics Research and Applications*, 20(3): 276-295. Available at: <https://doi.org/10.1080/13675567.2016.1219703>.
- Vadera, A.K., R.V. Aguilera and B.B. Caza, 2009. Making sense of whistle-blowing's antecedents: Learning from research on identity and ethics programs. *Business Ethics Quarterly*, 19(4): 553-586. Available at: <https://doi.org/10.5840/beq200919432>.
- Waytz, A., J. Dungan and L. Young, 2013. *The New York Times*, 1: SR12.
- Weiss, J.W., 2006. *Organization ethics*. 4th Edn., Ontario, CA: Thompson/South West.
- Wilde, J.H., 2013. Citizen watch in the accounting department? Tax and financial reporting responses to employee whistle-blowing allegations (Order No. 3608021). Available from ProQuest Dissertations & Theses Global. (1497226692).
- Windelberg, M., 2016. Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection*, 100(12): 4-11. Available at: <https://doi.org/10.1016/j.ijcip.2015.11.003>.

Views and opinions expressed in this article are the views and opinions of the author(s), International Journal of Management and Sustainability shall not be responsible or answerable for any loss, damage or liability, etc. caused in relation to/arising out of the use of the content.