Why Do Organizations Not Learn from Cybersecurity Crises? An Organizational Learning Perspective

Early stage paper

Hwee-Joo Kam
University of Tampa
hkam@ut.edu

Alaa Nehme
Mississippi State University
a.nehme@msstate.edu

Merrill Warkentin
Mississippi State University
m.warkentin@msstate.edu

ABSTRACT

Prior studies have established that organizations learn better from failure than from success. Nevertheless, cybersecurity crises resulting from cyberattacks tell a different story. It has been reported that some organizations have encountered repeat ransomware attacks, causing them to pay a second or even a third ransom. Due to the recurrences of cyberattacks, this study addresses organizations' failure to learn from not protecting their information assets. Many information systems (IS) studies have examined organizational learning in light of positive outcomes such as effective decision-making and management. On the other hand, this study addresses organizational learning by focusing on the negative aspects (i.e., the failures of preventing cyberattacks). In the near future, our research findings will share insights concerning the barriers of learning from cyberattack prevention failures, thereby expanding the 'Security, Education, Training, and Awareness' (SETA) perspective to incorporate organizational learning elements.

Keywords: organizational learning, cybersecurity crisis, learning from failures

INTRODUCTION

A cybersecurity crisis is a cyber disaster that have successfully obstructed an organization's key operations (Prevezianou 2021). While both information systems (IS) and management studies have suggested that organizations could learn from crises (Ahmad et al. 2019; Eismann et al. 2021; Kim 1998; Maitlis and Christianson 2014; Wang 2008; Wooten and James 2008), the reality of cybersecurity crises paints a different picture. A global report entitled "Ransomware Attacks and the True Cost to Business 2022" has revealed that 40% of its surveyed organization victims of ransomware attacks have paid a second ransom and 10% have paid a third ransom (Cybereason 2022). As organizational security practices play an important role to assure information security (Kam et al. 2021; Pérez-González et al. 2019), paying a second or a third ransom suggests that organizations have not really learned how to implement the right security practices.

Cybersecurity crises caused by massive cyberattacks may put organizations under immense time pressure for fast decision-making, suggesting that crisis impels organizations to make rapid decision for avoiding negative outcomes (Nunamaker et al. 1989). During the ransomware attack that forced Colonial Pipeline to shut down its digital systems, its CEO made a fast decision to pay around five million dollars of ransom in exchange of data release (Wilkie 2021). Cybersecurity crises will often impair key IS functions. For example, the 'WannaCry' ransomware paralyzed hospitals' IT systems in the United Kingdom, forcing them to delay delivering patients' care (Palmer 2017). Consistent with the notion that crises threaten organizational survival (Hale 1997), cybersecurity crises could paralyze organizations and bring organizations' operations to a halt.

The devastating effects of cybersecurity crises can be mitigated through crisis management (Ahmad et al. 2019; Housel et al. 1986). With good crisis management plans, cybersecurity crises can foster organizational learning (Ahmad et al. 2019) enhancing knowledge acquisition, information distribution and interpretation, and organizational memory (Huber 1991). Crises have propelled organizations to question their underlying principles, thus promoting organizational learning (Wang 2008). However, learning from crisis is not always a simple process (Antonacopoulou and Sheaffer 2014). In specific, organizational learning based on cybersecurity crises poses a unique challenge. This is mainly because one of the key components of cybersecurity – information technology (IT) – is complex in that IT infrastructure is usually linked to external systems to foster better collaboration with external constituents. The complex nature of IT creates difficulty in sensemaking (i.e., make sense of a current crisis) (Weick 1988), thus rendering organizational learning difficult. For example, it was hard to trace the cyberattack against SolarWinds which involved a supply chain system that distributed data to over 18,000 organizations (OWASP 2021). Moreover, cybersecurity crises usually transcend geo-political boundaries (Prevezianou 2021) and thus create complexities in sensemaking (e.g., find the attack point) (Ansell et al. 2010) which further complicates organizational learning (Dodgson 1993).

Since IT evolves rapidly, current security measures may become obsolete soon. Even with cutting-edge security measures, IT infrastructure may not be able to withstand cyberattacks against zero-day vulnerabilities (i.e., vulnerabilities that have yet been identified). For instance, a zero-day vulnerability called Log4J was exploited even in big organizations such as Google, Cisco, and Microsoft, compelling them to apply new security countermeasures (Kulkarni 2022). This suggests that technology operates in volatile environments fraught with cyber threats. So, organizations have to quickly "unlearn" the last obsolete countermeasures and learn new mechanisms to protect information assets. Unlearning itself is a complex process due to organizational biases and ingrained culture (Zahra et al. 2011). Eventually, the frequent actions of unlearning old elements and learning new elements may create complexities and challenges for consolidating organizational learning. In a cybersecurity context, such complexities encourage this study to examine the barriers of organizational learning. Hence, our first research question is:

RQ 1: What are the barriers for organizations to learn from cybersecurity crisis?

In the IS literature, numerous studies have addressed organizational learning in the context of software development (Fichman and Kemerer 1997; Lyytinen and Rose 2006; Salaway 1987; Stein and Vandenbosch 1996), business process outsourcing (Cha et al. 2008; Koo et al. 2017; Whitaker et al. 2010), and IT's role in learning (Goodman and Darr 1998; Janson et al. 2007; Kane and Alavi 2007; Robey et al. 2000; Schlagwein and Bjorn-Andersen 2014; Vandenbosch and Higgins 1995). All these studies share a common theme: using organizational learning to reach *positive* outcomes such as effective IS management. We argue that it is equally important to address organizational learning to shed light on the negatives. In specific, it is important to study failures of learning from information security safeguards, primarily because organizations learn better from failures than from successes (Madsen and Desai 2010). Nevertheless, IS studies related to this aspect are scarce. To fill this research gap, we address the following research question:

RQ 2: How can learning from a cybersecurity crisis in an organizational context be promoted?

The research contribution of this study is twofold. First, this study is expected to share the insights of organizational learning's obstacles in a cybersecurity context. By identifying the learning barriers, we can then share the mechanisms on how to overcome the barriers of learning from a cybersecurity crisis. Because cybersecurity attacks are ubiquitous, overcoming the barriers of learning becomes critical for organizations' information security. Second, learning in a cybersecurity context is usually related to Security, Education, Training, and Awareness (SETA). However, our research findings would provide a different perspective in that learning is not based only on security awareness training or cybersecurity education in general but also on the occurrences of real-life cybersecurity crises encountered by organizations. Accordingly, we argue that our research findings may contribute to the theoretical framework of SETA by showing how to incorporate organizational learning into SETA.

LITERATURE REVIEW

Cybersecurity Crises

Crises are multi-faceted, encompassing social-political, psychological, technological, and cognitive dimensions (Pearson and Clair 1998). According to Billings et al. (1980), a crisis poses high threats to organizations' values and profits, placing organizations under intense time pressure for rapid decision-making. In general, a crisis is characterized by high criticality, high uncertainties, high urgency, and rapid decision-making under enormous time pressure (Nunamaker et al. 1989; Pearson and Clair 1998). Although a given crisis has a low probability of occurrence, it could undermine organizational survival (Hale 1997).

We assert that cybersecurity crises are considered major parts of organizational crises mainly because cybersecurity crises caused by devastating cyberattacks (e.g., ransomware attack) would paralyze organizations' critical business functions and would eventually threaten organizational survival. This aligns with the definition of 'cyber crisis' (Prevezianou 2021). Moreover, cybersecurity crisis transcends geo-political boundaries (Prevezianou 2021), creating a transboundary circumstance that complicates sense-making and decision-making (Backman 2021). Because the property of being transboundary engenders a high degree of interdependency (Ansell et al. 2010), it would require collaborations of multiple parties (from different jurisdictions) to deescalate a crisis. Eventually, this adds tremendous challenges for organizations during crisis management.

In the IS literature, studies that addressed cybersecurity crises were presented in a context of cybersecurity incident response and emergency preparedness. Knight & Nurse (2020) conducted a qualitative study and proposed a crisis management framework to promote corporate communication during incident response. Built on Information Processing Theory, Naseer et al. (2021) ran a multiple case study to examine the role of business analytics in incident response management. Naseer et al. (2021) proposed that real-time analytics of organizations' IT infrastructure offers agility for organizations' cybersecurity incident response strategy. Moreover, Husák et al. (2022) suggested that the cybersecurity incident response team should iterate through the 'OODA' loop (Observe, Orient, Decide, Act) to increase situation awareness for effective incident handling. On the other hand, Lee & Kim (2020) empirically established that citizens from wealthier Europeans nations displayed a higher level of individual cybersecurity preparedness, whereas Kim & Lee (2021) revealed that attributes of incident responses such as apologies and excuses differed between United States and Korean organizations due to cultural differences.

Our literature review demonstrates that the extant IS literature does not really link crisis management or incident response handling to organizational learning for cyberattack prevention. To address this research gap, the following section presents a relation between cybersecurity crisis and organizational learning.

Organizational Learning

Organizational learning is defined as a process in which "*organizations build, supplement, and organize knowledge and routines around their activities within their cultures and adopt and develop organizational efficiency by improving the use of the broad skills of their workforces*" (Dodgson 1993, p. 377). The study of organization learning has been widely undertaken in IS studies. For instance, Salaway (1987) empirically established that organizational learning based on single-loop (i.e., identifying a problem) and double-loop (i.e., examining the underlying factors that contributed to a problem) learning (Argyris and Schön 1997) effectively enhanced the interactions between users and system analysts. On the other hand, Stein & Vandenbosch (1996) suggested that advanced system development such as developing expert systems offered ample opportunities for organizational learning. Additionally, Kane & Alavi (2007) examined the role of IT in organizational learning, proposing that the way IT tools were integrated, the way individuals used the tools, and the overall organizational environment affected organizational learning. Based on these IS studies, Templeton et al. (2002, p. 5) posited that organizational learning includes knowledge acquisition, information distribution, information interpretation, and organizational memory that would *"intentionally and unintentionally influence positive organizational change."* Consistent with Huber's (1991) conceptualization, Templeton et al.'s (2002) definition suggests that organizational learning embodies knowledge management.

Drawing on Argyris & Schön's (1997) organizational learning theory, Ahmad et al. (2019) proposed that an integrated framework of information security management and incident response planning enabled organizations to learn from cybersecurity crises. Particularly, cybersecurity crises offered opportunities for single-loop learning (i.e., identify the emerging problems such as detecting new attack vectors) and double-loop learning (i.e., question the underlying assumptions such as investigate the existing information security policies and strategies) (Ahmad et al. 2019). Conversely, several management studies presented barriers of learning from crisis. Also built on Argyris & Schön's (1997) theoretical framework, Smith & Elliott (2007) asserted that while *first-order learning* (i.e., single-loop learning) would often occur as organizations would most likely identify flaws in plans and procedures after going through a crisis, organizations might skip *second-order learning* (i.e., double-loop learning) by avoiding the examination of the underlying assumptions and by denying any wrongdoings. First-order learning is superficial, but second-order learning challenges the organizational norms and enables organizations to fundamentally assess their organizational systems (Smith and Elliott 2007). Bypassing second-order learning may deprive organizations the opportunities to uncover the key factors that contribute to crisis.

On the other hand, Madsen & Desai (2010) concluded that the major obstacles of learning from failure are caused by the difficulty in knowledge acquisition from the cyber incidents and by the political climate of “finger pointing”. In a cybersecurity context, the obstacles of learning may be even more convoluted. In addition to political climate, cybersecurity crises involve technology complexity. As stated earlier, the interconnectedness of IT infrastructure makes it hard to detect where an attack started. Even if organizations are able to identify the starting point of an attack, organizations may not be able to acquire knowledge, when, and how that attack occurred in an external component administered by their business associates. An example cited earlier, the ’SolarWinds’ attack, exemplified this difficulty. The attack against SolarWinds supply chain systems was first started by injecting arbitrary codes into a library that was digitally signed as legitimate and then executed during system updates (Williams 2020). The malicious codes were then propagated to different system components, installing backdoors that created system resources for active directory exploitation. Learning how this sophisticated attack actually works takes a special cognitive effort, and it will also become a challenge to learn how to prevent this type of attack from happening in the future. As stated by Weick (1988, p. 308):

> *“Unwitting escalation of crises is especially likely when technologies are complex, highly interactive, non-routine, and poorly understood. The very action which enables people to gain some understanding of these complex technologies can also cause those technologies to escalate and kill.”*

Leadership may also create barriers to learn from crises. Leadership could negatively influence organizational learning (Inkpen 1998; Ulrich et al. 1993; Yukl 2009) in that leaders might not encourage information sharing of an effective preventive measures across organizations. For example, an organizational unit learned a new security countermeasure, but the knowledge of countermeasure was not widely shared and implemented across organizations due to poor leadership approaches (e.g., leaders' discouragement of information sharing).

FUTURE RESEARCH

In conclusion, this study examines why and how organizations have failed to learn from the cybersecurity crises they have experienced. By analyzing the reasons behind organizations' failure to learn from previous cybersecurity crises, this study is expected to be prescriptive with relevant practical implications. In the near future, we plan to adopt a qualitative approach that will involve interviewing several Chief Information Security Officers (CISOs) whose organizations have experienced major cybersecurity attacks with devastating impacts. We will design semi-structured interview questions focusing on organizational learning from cybersecurity crises. Our questions will be informed by 'organizational learning' theory. Based on an in-depth review of theory, we will present a holistic framework that may explain organizational "non-learning" from cybersecurity incidents. After the analysis of our qualitative data, we will revisit our framework to develop a prescriptive model that addresses how organizations can learn from their victimization experiences. We plan to follow up with a second quantitative study that involves a survey and a test of a derived variance model from the framework.

Our research findings are expected to carry insights related to the barriers of organizational learning from cybersecurity crises and will offer suggestions on how to overcome these barriers.

Additionally, our research findings would present how to incorporate organizational learning into SETA, as we argue that the scope of SETA should be expanded to encompass a wider organizational context. We hope that our work-in-progress develops to shed light on the critical issue of organizational non-learning in the context of cybersecurity, and as such inform research, theory, and practice.

REFERENCES

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2019). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311

Ansell, C., Boin, A., and Keller, A. 2010. “Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System,” *Journal of Contingencies and Crisis Management* (18:4), pp. 195–207. (https://doi.org/10.1111/j.1468-5973.2010.00620.x).

Antonacopoulou, E. P., and Sheaffer, Z. 2014. “Learning in Crisis: Rethinking the Relationship Between Organizational Learning and Crisis Management,” *Journal of Management Inquiry* (23:1), SAGE Publications Inc, pp. 5–21. (https://doi.org/10.1177/1056492612472730).

Argyris, Ch., and Schön, D. A. 1997. “Organizational Learning: A Theory of Action Perspective,” *Monográfico Sobre La Formación y Las Organizaciones* (77:78), p. 345. (https://doi.org/10.2307/40183951).

Backman, S. 2021. “Conceptualizing Cyber Crises,” *Journal of Contingencies and Crisis Management* (29:4), pp. 429–438. (https://doi.org/10.1111/1468-5973.12347).

Billings, R. S., Milburn, T. W., and Schaalman, M. L. 1980. “A Model of Crisis Perception: A Theoretical and Empirical Analysis,” *Administrative Science Quarterly* (25:2), [Sage Publications, Inc., Johnson Graduate School of Management, Cornell University], pp. 300–316. (https://doi.org/10.2307/2392456).

Cha, H. S., Pingry, D. E., and Thatcher, M. E. 2008. “Managing the Knowledge Supply Chain: An Organizational Learning Model of Information Technology Offshore Outsourcing,” *MIS Quarterly* (32:2), Management Information Systems Research Center, University of Minnesota, pp. 281–306. (https://doi.org/10.2307/25148841).

Cybereason. 2022. "Report: Ransomware Attacks and the True Cost to Business 2022," A Global Study on Ransomware Business Impact. (https://www.cybereason.com/ransomware-the-true-cost-to-business-2022).

Dodgson, M. 1993. "Organizational Learning: A Review of Some Literatures," *Organization Studies* (14:3), SAGE Publications Ltd, pp. 375–394. (https://doi.org/10.1177/017084069301400303).

Eismann, K., Posegga, O., and Fischbach, K. 2021. "Opening Organizational Learning in Crisis Management: On the Affordances of Social Media," *The Journal of Strategic Information Systems* (30:4), 2021 Review Issue, p. 101692. (https://doi.org/10.1016/j.jsis.2021.101692).

Fichman, R. G., and Kemerer, C. F. 1997. "The Assimilation of Software Process Innovations: An Organizational Learning Perspective," *Management Science* (43:10), INFORMS, pp. 1345–1363. (https://doi.org/10.1287/mnsc.43.10.1345).

Goodman, P. S., and Darr, E. D. 1998. "Computer-Aided Systems and Communities: Mechanisms for Organizational Learning in Distributed Environments," *MIS Quarterly* (22:4), Management Information Systems Research Center, University of Minnesota, pp. 417–440. (https://doi.org/10.2307/249550).

Hale, J. 1997. "A Layered Communication Architecture for the Support of Crisis Response," *Journal of Management Information Systems* (14:1), Routledge, pp. 235–255. (https://doi.org/10.1080/07421222.1997.11518160).

Housel, T. J., El Sawy, O. A., and Donovan, P. F. 1986. "Information Systems for Crisis Management: Lessons from Southern California Edison," *MIS Quarterly* (10:4), Management Information Systems Research Center, University of Minnesota, pp. 389–400. (https://doi.org/10.2307/249195).

Huber, G. P. 1991. "Organizational Learning: The Contributing Processes and the Literatures," *Organization Science* (2:1), INFORMS, pp. 88–115. (https://doi.org/10.1287/orsc.2.1.88).

Husák, M., Sadlek, L., Špaček, S., Laštovička, M., Javorník, M., and Komárková, J. 2022. "CRUSOE: A Toolset for Cyber Situational Awareness and Decision Support in Incident Handling," *Computers & Security* (115), p. 102609. (https://doi.org/10.1016/j.cose.2022.102609).

Inkpen, A. C. 1998. "Learning and Knowledge Acquisition through International Strategic Alliances," *The Academy of Management Executive (1993-2005)* (12:4), Academy of Management, pp. 69–80.

Janson, M., Cecez-Kecmanovic, D., and Zupančič, J. 2007. "Prospering in a Transition Economy through Information Technology-Supported Organizational Learning," *Information Systems Journal* (17:1), pp. 3–36. (https://doi.org/10.1111/j.1365-2575.2006.00228.x).

Kam, H.-J., Kim, D. J., and He, W. 2021. "Should We Wear a Velvet Glove to Enforce Information Security Policies in Higher Education?," *Behaviour & Information Technology* (0:0), Taylor & Francis, pp. 1–15. (https://doi.org/10.1080/0144929X.2021.1917659).

Kane, G. C., and Alavi, M. 2007. "Information Technology and Organizational Learning: An Investigation of Exploration and Exploitation Processes," *Organization Science* (18:5), Linthicum, United States: Institute for Operations Research and the Management Sciences, pp. 796–812.

Kim, L. 1998. "Crisis Construction and Organizational Learning: Capability Building in Catching-up at Hyundai Motor," *Organization Science* (9:4), INFORMS, pp. 506–521. (https://doi.org/10.1287/orsc.9.4.506).

Kim, N., and Lee, S. 2021. "Cybersecurity Breach and Crisis Response: An Analysis of Organizations' Official Statements in the United States and South Korea," *International Journal of Business Communication* (58:4), SAGE Publications Inc, pp. 560–581. (https://doi.org/10.1177/2329488418777037).

Knight, R., and Nurse, J. R. C. 2020. "A Framework for Effective Corporate Communication after Cyber Security Incidents," *Computers & Security* (99), p. 102036. (https://doi.org/10.1016/j.cose.2020.102036).

Koo, Y., Lee, J.-N., Heng, C. S., and Park, J. 2017. "Effect of Multi-Vendor Outsourcing on Organizational Learning: A Social Relation Perspective," *Information & Management* (54:3), pp. 396–413. (https://doi.org/10.1016/j.im.2016.09.007).

Kulkarni, N. P. 2022. "Log4j Zero-Day Vulnerability: Everything You Need To Know About the Apache Flaw," *Spiceworks*, , February 16. (https://www.spiceworks.com/it-security/vulnerability-management/articles/log4j-apache-vulnerability-everything-you-need-to-know/, accessed June 28, 2022).

Lee, C. S., and Kim, J. H. 2020. "Latent Groups of Cybersecurity Preparedness in Europe: Sociodemographic Factors and Country-Level Contexts," *Computers & Security* (97), p. 101995. (https://doi.org/10.1016/j.cose.2020.101995).

Lyytinen, K., and Rose, G. M. 2006. "Information System Development Agility as Organizational Learning," *European Journal of Information Systems* (15:2), Taylor & Francis, pp. 183–199. (https://doi.org/10.1057/palgrave.ejis.3000604).

Madsen, P. M., and Desai, V. 2010. "Failing to Learn? The Effects of Failure and Success on Organizational Learning in the Global Orbital Launch Vehicle Industry," *Academy of Management Journal* (53:3), Academy of Management, pp. 451–476. (https://doi.org/10.5465/amj.2010.51467631).

Maitlis, S., and Christianson, M. 2014. "Sensemaking in Organizations: Taking Stock and Moving Forward," *Academy of Management Annals* (8:1), Academy of Management, pp. 57–125. (https://doi.org/10.5465/19416520.2014.873177).

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., and Masood Siddiqui, A. 2021. "Real-Time Analytics, Incident Response Process Agility and Enterprise Cybersecurity Performance: A Contingent Resource-Based Analysis," *International Journal of Information Management* (59), p. 102334. (https://doi.org/10.1016/j.ijinfomgt.2021.102334).

Naseer, H., Maynard, S. B., and Desouza, K. C. 2021. "Demystifying Analytical Information Processing Capability: The Case of Cybersecurity Incident Response," *Decision Support Systems* (143), p. 113476. (https://doi.org/10.1016/j.dss.2020.113476).

Nunamaker, J. F., Weber, E. S., and Chen, M. 1989. "Organizational Crisis Management Systems: Planning for Intelligent Action," *Journal of Management Information Systems* (5:4), Routledge, pp. 7–32. (https://doi.org/10.1080/07421222.1989.11517837).

OWASP. 2021. "A08 Software and Data Integrity Failures - OWASP Top 10:2021," Open Web Application Project. (https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/).

Palmer, D. 2017. "Hospitals across the UK Hit by WannaCrypt Ransomware Cyberattack, Systems Knocked Offline," *ZDNet*. (https://www.zdnet.com/article/hospitals-across-england-hit-by-cyber-attack-systems-knocked-offline/).

Pearson, C. M., and Clair, J. A. 1998. "Reframing Crisis Management," *Academy of Management Review* (23:1), Academy of Management, pp. 59–76. (https://doi.org/10.5465/amr.1998.192960).

Pérez-González, D., Preciado, S. T., and Solana-Gonzalez, P. 2019. "Organizational Practices as Antecedents of the Information Security Management Performance: An Empirical Investigation," *Information Technology & People* (32:5), Emerald Publishing Limited, pp. 1262–1275. (https://doi.org/10.1108/ITP-06-2018-0261).

Prevezianou, M. F. 2021. "Beyond Ones and Zeros: Conceptualizing Cyber Crises," *Risk, Hazards & Crisis in Public Policy* (12:1), pp. 51–72. (https://doi.org/10.1002/rhc3.12204).

Robey, D., Boudreau, M.-C., and Rose, G. M. 2000. "Information Technology and Organizational Learning: A Review and Assessment of Research," *Accounting, Management and Information Technologies* (10:2), pp. 125–155. (https://doi.org/10.1016/S0959-8022(99)00017-X).

Salaway, G. 1987. "An Organizational Learning Approach to Information Systems Development," *MIS Quarterly* (11:2), Management Information Systems Research Center, University of Minnesota, pp. 245–264. (https://doi.org/10.2307/249370).

Schlagwein, D., and Bjorn-Andersen, N. 2014. "Organizational Learning with Crowdsourcing: The Revelatory Case of LEGO," *Journal of the Association for Information Systems* (15:11). (https://doi.org/10.17705/1jais.00380).

Smith, D., and Elliott, D. 2007. “Exploring the Barriers to Learning from Crisis: Organizational Learning and Crisis,” *Management Learning* (38:5), SAGE Publications Ltd, pp. 519–538. (https://doi.org/10.1177/1350507607083205).

Stein, E. W., and Vandenbosch, B. 1996. “Organizational Learning during Advanced System Development: Opportunities and Obstacles,” *Journal of Management Information Systems* (13:2), Routledge, pp. 115–136. (https://doi.org/10.1080/07421222.1996.11518125).

Templeton, G. F., Lewis, B. R., & Snyder, C. A. (2002). Development of a Measure for the Organizational Learning Construct. *Journal of Management Information Systems*. http://www.tandfonline.com/doi/abs/10.1080/07421222.2002.11045727

Ulrich, D., Jick, T., and Glinow, M. A. V. 1993. “High-Impact Learning: Building and Diffusing Learning Capability,” *Organizational Dynamics* (22:2), pp. 52–66. (https://doi.org/10.1016/0090-2616(93)90053-4).

Vandenbosch, B., and Higgins, C. A. 1995. “Executive Support Systems and Learning: A Model and Empirical Test,” *Journal of Management Information Systems* (12:2), Routledge, pp. 99–130. (https://doi.org/10.1080/07421222.1995.11518083).

Wang, J. (2008). Developing Organizational Learning Capacity in Crisis Management. *Advances in Developing Human Resources*, *10*(3), 425–445. https://doi.org/10.1177/1523422308316464

Weick, K. E. 1988. “Enacted Sensemaking in Crisis Situations,” *Journal of Management Studies* (25:4), pp. 305–317. (https://doi.org/10.1111/j.1467-6486.1988.tb00039.x).

Whitaker, J., Mithas, S., and Krishnan, M. S. 2010. “Organizational Learning and Capabilities for Onshore and Offshore Business Process Outsourcing,” *Journal of Management Information Systems* (27:3), Routledge, pp. 11–42. (https://doi.org/10.2753/MIS0742-1222270302).

Wilkie, C. 2021. “Colonial Pipeline Paid $5 Million Ransom One Day after Cyberattack, CEO Tells Senate,” *CNBC*, , June 8. (https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html, accessed June 28, 2022).

Williams, J. 2020. *SANS Emergency Webcast: What You Need to Know about the SolarWinds Supply-Chain Attack - SANS Institute*. (https://www.sans.org/webcasts/emergency-webcast-about-solarwinds-supply-chain-attack-118015).

Wooten, L. P., and James, E. H. 2008. “Linking Crisis Management and Leadership Competencies: The Role of Human Resource Development,” *Advances in Developing Human Resources* (10:3), SAGE Publications, pp. 352–379. (https://doi.org/10.1177/1523422308316450).

Yukl, G. 2009. “Leading Organizational Learning: Reflections on Theory and Research,” *The Leadership Quarterly* (20:1), Leadership and Organizational Learning, pp. 49–53. (https://doi.org/10.1016/j.leaqua.2008.11.006).

Zahra, S. A., Abdelgawad, S. G., and Tsang, E. W. K. 2011. "Emerging Multinationals Venturing Into Developed Economies: Implications for Learning, Unlearning, and Entrepreneurial Capability," *Journal of Management Inquiry* (20:3), SAGE Publications Inc, pp. 323–330. (https://doi.org/10.1177/1056492611408266).