8-10-2022

Leading through the Crisis: What could CISOs do to Stop the Bleeding during a Cyberattack?

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

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

Leading through the Crisis: What could CISOs do to Stop the Bleeding during a Cyberattack?

TREO Talk Paper

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

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

Abstract

Cyberattacks, especially ransomware attacks, against organizations, have been spiking alarmingly. With ubiquitous cyberattacks, organizations have been on "pins and needles" trying to safeguard their information assets. Unfortunately, cyberattacks could still be inevitable. When a serious cyberattack exploits an organization's Information Technology (IT) infrastructure, leadership plays a critical role to reduce the organization's loss and restore its reputation. In the last four decades, literature in the management discipline has widely examined leadership roles in relation to crisis management (Farazmand, 2007; Weick, 1988; Yukl & Mahsud, 2010). In general, studies have reached consensus that adaptive, empathetic, and transformative leadership styles are conducive to crisis management.

A crisis reflects the "*points of indecision at which the central decision group believes it must make and implement the right decisions if the organization is to avoid significant negative outcomes – real or symbolic.*" (Nunamaker et al., 1989) In the context of Information Systems (IS), we argue that crises resulting from cyberattacks differ from traditional crises undergone due to four reasons. First, since cybersecurity is a relatively new field, executives may not be able to refer to the prior crisis management that have proven effective. That is, executives may find it hard to search for a "textbook" case that shows what not to do during a cybersecurity crisis. Second, the constant changes in technology may create volatility, affording only a "small window" for executives to make strategic decisions (Eisenhardt, 1989). Third, cybersecurity crises caused by ransomware attacks may have long-lasting negative impacts on organizations. For instance, in the event of a ransomware attack, an organization's payment to attackers to retain control of its data does not necessarily end the event as attackers may secretly run a post exploitation attack that may involve installing a backdoor for persistence threat. This may affect incident response handling as part of crisis management. Finally, cybersecurity is complex by nature. IT infrastructure is usually connected to some external systems to foster better collaboration with external constituents. Such interconnectedness may pose a problem during a crisis in such a way that it may be challenging to pinpoint the "starting point" and the endpoint of a cyberattack. As a result, it may be hard to isolate a software component that has been compromised. Such technical complexities pose a challenge to crisis management.

Because crisis management corresponds to leadership (Weick, 1988), we develop a model that explains what leadership styles contribute to effective managerial approaches in minimizing the damage during a disastrous cyberattack. In other words, the model offers insights into what type(s) of leadership would best help "stop the bleeding" when organizations are hit by cybersecurity attacks. In our model development, we offer several propositions that unveil why and what leadership styles are related to effective crisis management in the event of a cyberattack. The implications are discussed.

References

Eisenhardt, K. M. (1989). Making Fast Strategic Decisions in High-Velocity Environments. *Academy of Management Journal*, *32*(3), 543–576. https://doi.org/10.5465/256434

Farazmand, A. (2007). Learning from the Katrina Crisis: A Global and International Perspective with Implications for Future Crisis Management. *Public Administration Review*, *67*(s1), 149–159

Nunamaker, J. F., Weber, E. S., & Chen, M. (1989). Organizational Crisis Management Systems: Planning for Intelligent Action. *Journal of Management Information Systems*, *5*(4), 7–32.

Weick, K. E. (1988). Enacted Sensemaking in Crisis Situations. *Journal of Management Studies*, *25*(4), 305–317.

Yukl, G., & Mahsud, R. (2010). Why Flexible and Adaptive Leadership is Essential. *Consulting Psychology Journal: Practice and Research*, *62*(2), 81–93. https://doi.org/10.1037/a0019835