Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2018 Proceedings | Midwest (MWAIS)

5-2018

Toward Cybersecurity Leadership Framework

Simon Cleveland
City University of Seattle, simoncleveland@cityu.edu

Marisa Cleveland
Northeastern University, cleveland.m@husky.neu.edu

Toward Cybersecurity Leadership Framework

Simon Cleveland
City University of Seattle
simoncleveland@cityu.edu

Marisa Cleveland
Northeastern University
cleveland.m@husky.neu.edu

ABSTRACT

Cybersecurity is a critical issue for organization and executive leadership faces challenges that their predecessors escaped. If executive leadership and boards of directors are charged with setting policy and regulations regarding the company's cybersecurity efforts, a greater understanding of the field and the threats needs to be communicated before leadership can be expected to make critical decisions in the face of cyberattacks. This study addresses what type of leadership should be applied in the various cybersecurity preparation and response stages in order to educate cybersecurity leaders in developing a prescriptive approach to addressing future cyberattacks. A novel cybersecurity leadership framework is proposed, which recommends leadership styles against the functional areas of the cybersecurity preparation and response stages.

Keywords

Cybersecurity framework, leadership theory, cyber skills

INTRODUCTION

There is a gap between the level of knowledge regarding cybersecurity and the amount of information the executive leadership has in making informed decisions regarding cybersecurity. While cybersecurity is a critical issue for all companies in today's digital landscape, executive leadership faces challenges that their predecessors escaped. If executive leadership and boards of directors are charged with setting policy and regulations regarding the company's cybersecurity efforts, a greater understanding of the field and the threats needs to be communicated before leadership can be expected to make critical decisions in the face of cyberattacks. Auffret et al. (2017) argued that "cybersecurity is widely viewed as a matter of pressing national importance" (p. 2). In the last half a decade, cyberattacks have become more visible to the public. The threats and the attacks call for a more proactive approach from leadership; however, when risk management fails, the leaders need to be prepared to handle the incidents after they occur. While U.S. Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported nearly 300 incidents against U.S. industrial control systems in 2015 (Auffret et al., 2017), in 2016 the Identity Theft Resource Center saw a 40% increase in the total number of breaches. Extant literature has focused primarily on technology measures to prevent cybersecurity incidences (Holstein, Cease & Seewald, 2015; Knowles et al., 2015), but there is a gap in literature that addresses appropriate leadership skills required for each of the stages in a cybersecurity incident preparation and response.

As a result, this study attempts to address the question: what type of leadership should be applied in the various cybersecurity preparation and response stages in order to educate cybersecurity leaders in developing a prescriptive approach to addressing future cyberattacks? To address the research question, we leverage the existing cybersecurity frame proposed by the National Institute of Standards and Technology (NIST). We analyze leadership theory to highlight the various leadership styles and map these styles against the NIST framework. Finally, we propose a novel cybersecurity leadership framework that recommends leadership styles against the functional areas of the cybersecurity preparation and response stages. The paper concludes with recommendations for future research.

CYBERSECURITY VULNERABILITIES - THE NEED FOR A FRAMEWORK

In 2016, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a component of the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC), reported over 2,300 vulnerabilities from security researchers, vendors, and public sources (ICS-CERT, 2016). To respond to these vulnerabilities, the team released 185 advisories and 17 alerts. The sectors that received the highest vulnerability impacts were energy, critical manufacturing, commercial facilities, and water and wastewater systems. In 2017, the ICS team conducted over 170 assessments (a 35% increase compared to 2016) to determine the state of readiness of the United States' critical infrastructure against cyberattacks (ICS-CERT, 2017). The team's report showed that the most prevalent weaknesses included boundary protection, identification and authentication, allocation of resources, physical access control, account management, and least functionality.

Recognizing the ongoing threat to the United States' critical infrastructure, NIST released a preliminary cybersecurity framework in October of 2013 and then formalized it in 2014, to help organizations limit cybersecurity risks (Robertson, 2014; NIST, 2014). The framework is intended to help leaders improve their organization's cyber resiliency, determine the state of their cybersecurity readiness, assess potential gaps and risks, and recommend specific tools to address potential threats (NIST, 2014). The framework consists of several core functional areas as identified in Table 1.

To date, the focus of the framework has been to use specific drivers to consider the cybersecurity risks and lead cybersecurity activities of each organization (NIST, 2014); however, it doesn't provide a prescriptive approach as to what leadership skills apply to each of the proposed core functional areas.

CYBERSECURITY LEADERSHIP

Tubbs and Schulz (2006) define leadership as the individuals that influence others in order to achieve the goals of the organization. Leadership is essential for the success of any organization, and without it, companies would not meet their objectives to deliver products and services to their customers. As with managerial styles, literature identifies a myriad of leadership styles. One leadership theory is the theory X. It argues that such leaders believe that employees need to be constantly micromanaged to ensure their duties are performed and no detail is left out. In contrast, the theory Y leader is someone who doesn't need to remind employees that work needs to be completed, but rather nurtures these employees and helps them advance their careers (Northouse, 2017).

Function Area	Description	Categories
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.	Access Control Awareness and Training Data Security Information Protection Processes and Procedures Maintenance Protective Technology
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.	Anomalies and Events Security Continuous Monitoring Detection Processes
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event.	Response Planning Communications Analysis Mitigation Improvements
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event.	Recovery Planning Improvements Communications

Table 1. NIST Cyber Security Framework (adapted from NIST, 2014).

Leaders of organizations in today's cybersecurity environment should be accustomed to receiving the four a.m. phone call regarding a cyber crisis, and to manage this crisis they need to use a set of skills unprecedented in the current digital economy. Moreover, how they manage a crisis related to a cyberattack will depend on the type of leader they are, since cyberattacks will have an impact on the whole organization.

Leadership awareness and response to cyberattacks requires a set of best practices for immediate solutions. By the time a cyberattack has occurred, leadership will be unable to respond with preventative measures. Even with robust and resilient controls in place, the global nature of information technology systems makes the response in the moments after a cyberattack much more than technological. The response from leadership must be obtained by recognizing a broad scope of factors: behavior, culture, socioeconomic context, and a single organization or across multiple organizations. Auffret et al. (2017) argued that many of these factors have led to the creation of the Chief Information Security Officer (CISO) role in

organizations. The leader in this role is responsible for the strategic planning and implementation of the cybersecurity programs that can enhance the defense of the organization against cyber threats. As such, the person in this role needs to have power and authority to assemble the required resources in place to make the program a success, while taking into account the variety of factors that can have negative impacts on the implementation of the program. As a result, this CISO as a leader needs to possess not only technical skills, but also business acumen, resilience, and team building skills.

In addition the proposed skills, Sinha et al. (2015) argued that leaders should establish a strong Stackelberg equilibrium. This concept, proposed by Leitmann (1978), suggests that a leader should be "capable of inducing a favorable equilibrium by selecting a strategy arbitrarily close to the equilibrium that causes the follower to strictly prefer the desired strategy" (p.20). In other words, leaders should possess a strategic acumen in order to impact the strategies of their followers. With regards to the cybersecurity arena, such leaders can use both inspirational vision and incentive structure (Hult & Sivanesan, 2013). When it comes to a vision that inspires the followers, leaders should be cognizant of the set of organizational values in order to build cyber resilience. To influence the behaviors of individuals, these leaders can incentivize them in order to construct a cybersecurity mindset. Bass (1988) argued that the inspiring leader is perceived by others to be someone who has knowledge and sensitivity to the problems that need to be addressed. Furthermore, an inspiring leader is not someone who micromanages and forces others to follow, but is the one who guides (Morareschu, 2009). Inspiring leaders are above all passionate about helping others in their organizations.

One of the most distinct qualities of an inspirational leader is his or her passion to help others. This type of quality is associated more closely with servant leadership. According to Albright (2016) "to lead effectively, we must first serve, and that means the legitimate needs of others is the essence of what it means to serve" (Albright, 2016, p. 19). This quality focuses on the employees and their development. Leading is a form of guiding and supporting, understanding, being genuine, developing relationships, and building a community (Cleveland & Cleveland, 2018). Albright identifies servant leadership as leaders investing in their employees and breaks down servant leadership into four key values: inspiration, equality, community incorporation, and guidance (2016). By investing in employees, servant leaders encourage and support their employees to hone in on their successes, instead of the leader's success. In organizations, servant leaders would be effective in helping their employees adapt to change by learning how the employees process things, and together, work on ways to integrate better within the organization. The practice of servant leadership is often characterized with positive results, such as decreased employee turnover (a major inhibitor for company success), improved job satisfaction, and employee loyalty. Inspirational leaders who practice such qualities will ensure that their organizations create a safe place where employees remain committed to the mission of the organization and motivated to follow its vision.

In addition to passion to help others, inspiring leaders are also competent leaders. Competence is a kind of thirst for knowledge and self-improvement that demonstrates skills needed to overcome challenges. De Pree (2002) argued that competent leaders are transforming leaders. Transformational leaders stimulate their followers' efforts "to be innovative and creative by questioning assumptions, reframing problems, and approaching old situations in new ways," (Avolio & Bass, 2002, p. 2). Transformational leadership focuses on transforming employees since such "leaders who truly excel are those who transform results, performance, and culture" (Galloway, 2016). Transformational leadership focuses on tasks that help understand what motivates and influences employees, how to coach employees to improve performance, how to help employees understand strategy, how to measure what employees want, monitors employee progress, and assesses value rather than numbers" (Galloway, 2016). This seems to be an approach of "transforming" the employee to "value" organizational goals. Transitional leaders "want to help others see value in the goals and leverage what others are interested in or motivated by," (Galloway, 2016).

A key quality for inspiring leaders is mentorship. Knapp (2015) argued that "Leaders are mentors who focus on developing strong relationships with organization members," (p. 856). This quality instills in a leader to guide, mentor, and provide feedback to the manager to help him/her see their actions from another perspective. Furthermore, this quality helps a leader to build trust with the employees through feedback and guidance. Another leadership style is the authentic leadership. These types of leaders are self-aware, mission-driven and focused on the long-term results (Hewitt, 2015). Yet another style is the adaptive leadership. This style proposes that leaders adapt to the situation at hand in order to mobilize employees to address difficult scenarios and succeed (Heifetz, Grashow & Linsky, 2009). Such leaders are persistent, methodical, and able to accept disequilibrium and discomfort. Hult and Sivansen (2013) also argued that cybersecurity leadership needs to be focused on the mission. They noted that "The mission when clearly articulated builds a shared sense of purpose throughout the cyber security function and extends beyond into the wider organization," (p. 116). Finally, Karaman, Çatalkaya, and Aybar (2016) argued that when it comes to crisis response, leaders should strive to build a resilient command and control structure in order to minimize harm.

PROPOSED CYBERSECURITY LEADERSHIP FRAMEWORK

The leadership styles identified in the literature review are mapped against the cybersecurity framework proposed by NIST. Table 2 identifies the appropriate leadership styles necessary to address each core functional area.

Function Area	Leadership Theory and Style	Sources
Identify	Adaptive; Authentic; Theory Y; Servant; Inspirational; Mentorship	Albright (2016) ; Bass (1988); Heifetz, Grashow & Linsky (2009); Hewitt (2015); Hult & Sivanesan (2013); Knapp (2015); Morareschu (2009); Northhouse (2017);
Protect	Adaptive; Theory X; Inspirational; Transformational; Mentorship	Avolio & Bass (2002); Bass (1988); De Pree (2002) ;Galloway (2016);Heifetz, Grashow & Linsky (2009); Hult & Sivanesan (2013); Knapp (2015); Morareschu (2009);
Detect	Adaptive; Inspirational; Transformational; Mentorship	Avolio & Bass (2002); Bass (1988);De Pree (2002); Galloway (2016);Heifetz, Grashow & Linsky (2009);Hult & Sivanesan (2013);Knapp (2015); Morareschu (2009);
Respond	Adaptive; Authentic; Inspirational; Resilient; Stacklberg equilibrium; Mentorship	Bass (1988); Hewitt (2015); Heifetz, Grashow & Linsky (2009);Hult & Sivanesan (2013); Morareschu (2009); Karaman, Çatalkaya & Aybar (2016); Knapp (2015); Leitmann (1978); Singha et al. (2015)
Recover	Adaptive; Authentic; Inspirational; Servant; Transitional; Mentorship	Albright (2016) ; Bass (1988);Heifetz, Grashow & Linsky (2009); Hewitt (2015); Hult & Sivanesan (2013);Knapp (2015); Morareschu (2009);

Table 2. Proposed Cyber Security Leadership Framework

CONCLUSION

This study addressed the question: what type of leadership should be applied in the various cybersecurity preparation and response stages in order to educate cybersecurity leaders in developing a prescriptive approach to addressing future cyberattacks? Analysis of the existing cybersecurity framework proposed by NIST was conducted. Moreover, a review of the leadership theories was proposed to highlight the various leadership styles. Finally, these styles were mapped against the NIST framework to develop a new cybersecurity leadership framework. Future research will validate this framework through quantitative study among cybersecurity leaders.

REFERENCES

1. Albright, M. (2016). Servant leadership: Not just buzzwords. *Strategic Finance*, 98(4), 19-20.
2. Auffret, J. P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., ... & Warweg, P. (2017). Cybersecurity Leadership: Competencies, Governance, and Technologies for Industrial Control Systems. *Journal of Interconnection Networks*, *17*(01), 1740001.
3. Avolio, B. J., & Bass, B. M. (Eds.). (2001). Developing potential across a full range of Leadership Tm: Cases on transactional and transformational leadership. Psychology Press.
4. Bass, B. (1988). The inspirational processes of leadership. *Journal of Management Development*, *7*(5), 21-31.

5. Cleveland, M. & Cleveland, S. (2018). Toward understanding the impact of entrepreneurial leadership skills on community engagement. *Proceedings of the 6th International Conference on Innovation and Entrepreneurship*, Washington, DC, 15-22.
6. De Pree, M. (2002). Servant-leadership: Three things necessary. *Focus on leadership: Servant leadership for the*, *21*, 89-100.
7. Galloway, S.M. (2016). What makes a leader transformational? *Leadership excellence*, 33(5), 20-21.
8. Heifetz, R. A., Grashow, A., & Linsky, M. (2009). The practice of adaptive leadership: Tools and tactics for changing your organization and the world. Harvard Business Press.
9. Hewitt, F. (2015). Authentic leadership. *NZ Business + Management*, 29(8), M16-M17.
10. Holstein, D., Cease, T. W., & Seewald, M. G. (2015, September). Application and Management of Cybersecurity Measures for Protection and Control. In *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2015 International Conference on* (pp. 76-83). IEEE.
11. Hult, F., & Sivanesan, G. (2014). What good cyber resilience looks like. *Journal of business continuity & emergency planning*, *7*(2), 112-125.
12. ICS-CERT. (2016). ICS-CERT annual vulnerability coordination report. Retrieved on February 6, 2018 from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf ICS-CERT. 2017.
13. ICS-CERT Monitor (2017). Retrieved on February 7, 2018 from https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Nov-Dec2017_S508C.pdf
14. NIST. (2014). Framework for improving critical infrastructure cybersecurity. Retrieved on February 6, 2018 from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
15. Karaman, M., Çatalkaya, H., & Aybar, C. (2016). Institutional Cybersecurity from Military Perspective. *International Journal of Information Security Science*, *5*(1), 1-7.
16. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80.
17. Knapp, S. (2015). Lean Six Sigma implementation and organizational culture. *International journal of health care quality assurance*, *28*(8), 855-863.
18. Leitmann, G. (1978). On generalized Stackelberg strategies. *Journal of optimization theory and applications*, *26*(4), 637-643.
19. Morarescu, D. (2009). New look, new leadership. *Oncology Nursing e-Mentorship Program. Newsletter*, 1-8.
20. National Institute of Standards and Technology (NIST). (2014). Framework for improving critical infrastructure cybersecurity (version 1.0). Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
21. Northouse, P. G. (2017). *Introduction to leadership: Concepts and practice*. Sage Publications.
22. Tubbs, S. L., & Schulz, E. (2006). Exploring a taxonomy of global leadership competencies and meta-competencies. *Journal of American Academy of Business*, *8*(2), 29-34.