5-2018

Cybercrime Post-Incident Leadership Model

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

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

Cybercrime Post-incident Leadership Model

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

Simon Cleveland
City University of Seattle
simoncleveland@cityu.edu

ABSTRACT

Cybercrimes are facts of the modern technological society. While extant literature proposes a variety of prescriptive practices to combat cybercrimes, there is scant research to address how organizational leaders should minimize the impact of cybercrimes on their companies and the community after they have occurred. This study addresses the steps leaders should take in the aftermath of cybercrimes and proposes a four-stage leadership model consisting of best practices to guide leaders in preparing, responding, and recovering from a digital or cybersecurity attack.

Keywords

Cyber leadership, post-incident, cybercrimes, cyber breaches

INTRODUCTION

Cybercrimes, cybersecurity, and cyber forensics address the awareness and risks for organizations in today's modern digital landscape. Organizations do not plan to fail, but as businesses utilize technology to compete in the marketplace, corporate hacks and data breaches occur. Plenty of research has been done regarding how to prevent cybercrimes, how to increase cybersecurity, and how to analyze the cyber forensics component in the aftermath, but there is a gap in literature addressing organizational digital crimes and how leadership minimizes risk for the consumer and the organization. Cybersecurity is no longer solely an issue for the IT department, and leaders need to prepare their procedures for combatting the ever-evolving risks (Mccollum, 2012).

Emergency plans—whether natural disaster or cybercrime—should be regularly updated. As a result, this paper aims to address the question: what steps should leaders take in the aftermath of cybercrimes? To address this question, a four-stage leadership model consisting of best practices is proposed to guide leaders in preparing, responding, and recovering from a digital or cybersecurity attack.

CYBER BREACHES

In today's modern digital landscape, organizations are vulnerable to cybercrime. For example, in 2013, the Target stores data breach affected 70 million people (Manworren, Letwat, & Daily, 2016), while in 2015, the Anthem Health Insurance hack affected 80 million people (MacIntyre et al., 2017). With the Equifax breach in 2017, 143 million people were affected (Moore, 2017), and Yahoo's 2013 cybersecurity failure resulted in 1 billion breached accounts (Cheng, Liu, & Yao, 2017). This data indicates that no single industry is the primary targeted; however, common denominators in every company include a leadership team and digital presence. Furthermore, it is unlikely and nearly impossible for companies to remove themselves from the internet. Yet, despite all the preparation, cybercrime still remains a major concern for every industry.

Challenges of Managing Cybercrimes

Computer-related crimes have three distinct categories: input tampering, throughput tampering, and output tampering. While input scams are the most common computer-related crime, it is also the easiest kind to prevent by utilizing effective supervision and controls. Throughput crimes are rarer, due to the programming knowledge required, but output crimes are increasing, and these involve theft of computer-related reports and information files (Ionescu, Mirea, & Blajan, 2011).

Staff constraints and lack of training for digital crimes suggest law enforcement investigation resources will be thin. As a result, company leaders need to recognize the challenges and limitations placed upon law enforcement (Gogolin & Jones, 2010). According to Gogolin and Jones (2010), most law enforcement officers chose their profession for traditional law enforcement, as opposed to dealing with cybercrimes, leaving the FBI as the sole federal agency to handle cybercrimes.

Cybersecurity Risk Management

With the rapid pace of technology changing the way consumers behave, corporate executives are charged with the responsibility of producing more and staying ahead of the trends. Managing risks associated with cybercrimes requires a commitment from leadership to pursue ongoing training in order to acquire up-to-date knowledge and skills. Scammers and hackers continue to hone their craft and develop workarounds to complement the new technology. Leadership in organizations needs to understand the complexity of cyberattacks and the resources it will take to prevent them and adopt a prescriptive approach to cybersecurity risk management (Paté-Cornell et al., 2018).

Cyber Forensics

Law enforcement and digital forensic teams need to work collaboratively to collect, preserve, examine, and transfer digital evidence in a timely and accurate manner. For example, Bulbul, Yavuzcan, and Ozel (2013) proposed a crime scene procedure model in order to ensure a standardization among all professionals interacting with the investigation. Similarly, Montasari, Peltola, and Evans (2015) proposed an integrated computer forensics investigation process model (ICFIPM) to assist in the detection of computer crime investigations. Such models offer generalized guidelines that cyber forensic teams can leverage to address cybercrimes.

FOUR-STAGE CYBERCRIME LEADERSHIP MODEL

According to Mccollum (2012), digital crimes are on the rise, and cyberattacks are a top economic crime. Bhattacharya (2011) examined information security issues within small businesses and found a significant correlation between leadership styles and the level of concern toward information security problems within small businesses. Ineffective leadership styles can lead to businesses needing to take reactive measures against cybercrime. As organizations become increasingly dependent on information systems, leaders in all industries must recognize the issue of cybersecurity. According to Gupta and Hammond (2005), organizations with strong leaders engaged in more preventive efforts than organizations with weaker support from higher management.

Once an organization is the victim of a cybercrime, best practices for leaders in the aftermath need to be developed and documented. A four-stage model consisting of a set of processes is proposed to guide leaders during the aftermath of cybercrimes.

Stage 1: Recognizing Vulnerabilities

Events of a crisis typically unfold quickly, by the minute rather than the hour. After a cybercrime has occurred, leaders need to recognize and take ownership of the problem. Even as they rely on their teams, they should insert themselves into the process, intervening early and often. Berghel (2014) addressed the leadership failures in the National Security Complex and argued that leadership is the root of the cybersecurity problem. Turning a blind eye or ignoring existing vulnerabilities will result in a greater impact of the cybercrime and more lasting effects (Fischbacher-Smith, 2015).

Stage 2: Executing a Crisis Management Plan

Crisis management plans save valuable time by delegating tasks and providing critical information (Avery, Graham, & Park, 2016). Leadership in today's digital age, particularly effective cybersecurity leadership, is complex and involves a technical, legal, and ethical skillset (Berghel, 2014). Leadership after a cyberattack should be prepared to immediately respond with a well-prepared crisis management plan. Leaders need to decide if operations can resume immediately or if there is a contingency plan in place. According to Kowalski (2018), crisis management plans should be developed by the company's leadership team along with asset managers, legal counsel, and insurance providers.

Stage 3: Educating the Community

After the Exxon-Valdez Oil Spill in March of 1989, 11 million gallons of crude tanker oil were spilled into the Prince William Sound of Alaska (Cohen, 1995). The Mayor of Valdez led no major clean-up effort. Furthermore, the Exxon CEO failed to make a public statement until two weeks after the spill.

In contrast, during the BP oil spill in April of 2010, an explosion on Deepwater Horizon oil rig in the Gulf of Mexico near Louisiana killed 11 people, injured 16, and leaked an estimated 210 million gallons of oil over the course of 87 days (Mills & Koliba, 2016). The CEO of BP released a video to the public apologizing for the spill and BP's actions, provided updates on the clean-up, and committed to assist financially for the next 50 years.

To help combat digital crimes, leaders should adopt BP's approach and become the voice of reason and display resiliency (Armour, 2017). Leaders need to adopt an entrepreneurial approach to uniting communities through social capital (Cleveland

& Cleveland, 2018). Their goal should be to commit relentlessly and honestly to the populace throughout the crisis. To accomplish this, they should leverage news conferences giving clean-up tips and plans for up-to-the-minute progress reports to build trust in your leadership. Moreover, there should be a constant feedback mechanism to ensure that the information being disseminated is absorbed and acted upon properly (Goldes et al., 2017).

Stage 4: Conducing After Action Reviews

Leaders should study the lessons learned from prior victims of cybercrimes. Such lessons can be leveraged as action plans and best practices (Cleveland, 2012). Leaders should adopt strategies based on the most proven approaches that have worked for cybercrime victims in the past. These strategies can help organizations recover quicker and minimize the overall impact of the crimes. Furthermore, leaders should not overlook those who might not have a strong voice in their organizations and take care not to shut out others due to a difference of views or opinions. Rather, leaders should utilize after action reviews with their employees to brainstorm plausible actions to solve a cybercrime as soon as possible (Ariely, 2014). These reviews should involve reviews of the cyber incident, immediate institution of changes, and lessons on how to improve in the future.

Figure 1 summarizes the four-stage model as proposed in this study.

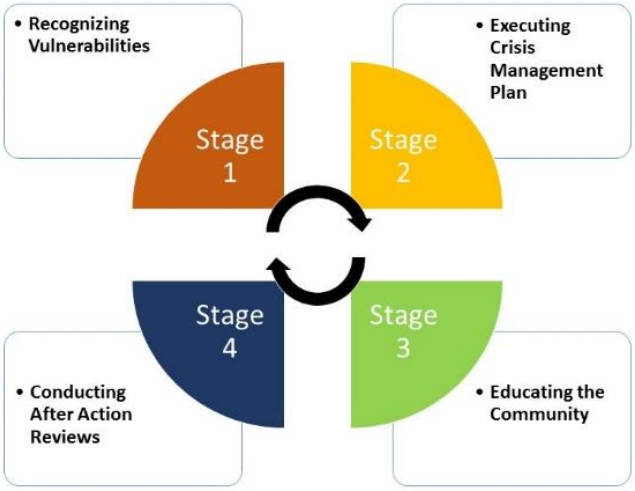

Figure 1. Four-stage leadership model during the aftermath of cybercrimes

CONCLUSION

Competent leadership in a time of crisis is essential. Whether a natural disaster or a cyberattack, citizens are affected and lives are changed. This paper attempts to address the question: what steps should leaders take in the aftermath of cybercrimes? To do so, it proposed a four-stage leadership model consisting of best practices to assist leadership actions post-incident of cybercrimes. Future research will validate the model using a qualitative study of leaders before and after the occurrence of cybercrimes.

REFERENCES

1. Ariely, G. A. (2014). Adaptive Responses to Cyberterrorism. In *Cyberterrorism* (pp. 175-195). Springer, New York, NY.
2. Armour, C. (2017). Cyber resilience: Leadership matters. *Cyber Security: A Peer-Reviewed Journal*, *1*(2), 134-146.

3. Avery, E. J., Graham, M., & Park, S. (2016). Planning makes (closer to) perfect: exploring United States' local government officials' evaluations of crisis management. *Journal of Contingencies and Crisis Management*, *24*(2), 73-81.

4. Berghel, H. (2014). Leadership failures in the national security complex. *Computer*, *47*(6), 64-67.

5. Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security*, *19*(5), 300-312.

6. Bulbul, H. I., Yavuzcan, H. G., & Ozel, M. (2013). Digital forensics: an analytical crime scene procedure model (ACSPM). *Forensic science international*, *233*(1-3), 244-256.

7. Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5).

8. Cleveland, S. (2012). Using microblogging for lessons learned in information systems projects. In *Workshop on IT Project Management*, 1-5.

9. 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.

10. Cohen, M. J. (1995). Technological disasters and natural resource damage assessment: an evaluation of the Exxon Valdez oil spill. *Land Economics*, 65-82.

11. Fischbacher-Smith, D. (2015). The enemy has passed through the gate: Insider threats, the dark triad, and the challenges around security. *Journal of Organizational Effectiveness: People and Performance*, *2*(2), 134-156.

12. Gogolin, G., & Jones, J. (2010). Law enforcement's ability to deal with digital crime and the implications for business. *Information Security Journal: A Global Perspective*, *19*(3), 109-117.

13. Goldes, S., Schneider, R., Schweda, C. M., & Zamani, J. (2017, June). Building a viable information security management system. In *Cybernetics (CYBCONF), 2017 3rd IEEE International Conference on* (pp. 1-6). IEEE.

14. Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information management & computer security*, *13*(4), 297-310.

15. Ionescu, L., Mirea, V., & Blajan, A. (2011). Fraud, corruption and cyber crime in a global digital network. *Economics, Management and Financial Markets*, *6*(2), 373.

16. Kowalski, B. (2018, January 30). Smart strategies for effective crisis management. Property and Casualty360. Retrieved on February 18, 2018 from http://www.propertycasualty360.com/2018/01/30 /smart-strategies-for-effective-crisis-management

17. MacIntyre, C. R., Engells, T. E., Scotch, M., Heslop, D. J., Gumel, A. B., Poste, G., ... & Broom, A. (2017). Converging and emerging threats to health security. *Environment Systems and Decisions*, 1-10.

18. Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*(3), 257-266.

19. Mccollum, T. (2012). Digital crimes on the rise: now that cyberattacks are a economic crime, they need to be on every organization's radar. *Internal Auditor*, *69*(1), 13-15.

20. Mills, R. W., & Koliba, C. J. (2015). The challenge of accountability in complex regulatory networks: The case of the Deepwater Horizon oil spill. *Regulation & Governance*, *9*(1), 77-91.

21. Montasari, R., Peltola, P., & Evans, D. (2015, September). Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations. In *International Conference on Global Security, Safety, and Sustainability* (pp. 83-95). Springer, Cham.

22. Moore, T. (2017). On the harms arising from the Equifax data breach of 2017. *International Journal of Critical Infrastructure Protection*, *19*, 47-48.

23. Paté-Cornell, M., Kuypers, M., Smith, M., & Keller, P. (2018). Cyber Risk management for critical infrastructure: a risk analysis model and three case studies. *Risk Analysis*, *38*(2), 226-241.