

Association for Information Systems

AIS Electronic Library (AISeL)

SAIS 2023 Proceedings

Southern (SAIS)

7-1-2023

Improving Organizational Cybersecurity Efforts through the Application of High-Reliability Organizing Concepts

Clay Posey

AJ Burns

Follow this and additional works at: <https://aisel.aisnet.org/sais2023>

Recommended Citation

Posey, Clay and Burns, AJ, "Improving Organizational Cybersecurity Efforts through the Application of High-Reliability Organizing Concepts" (2023). *SAIS 2023 Proceedings*. 28.
<https://aisel.aisnet.org/sais2023/28>

This material is brought to you by the Southern (SAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in SAIS 2023 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

IMPROVING ORGANIZATIONAL CYBERSECURITY EFFORTS THROUGH THE APPLICATION OF HIGH-RELIABILITY ORGANIZING CONCEPTS

Clay Posey

Brigham Young University
clay.posey@byu.edu

AJ Burns

Louisiana State University
ajburns@lsu.edu

ABSTRACT

Despite significant efforts to limit organizations' exposure to and harm caused by cybersecurity events, such incidents continue to abound. One foundation whose concepts—if applied—could help substantially improve organizational cybersecurity efforts is high-reliability organizing. Focused on how organizations operate in volatile environments yet maintain high levels of reliability, this literature provides meaningful insights to events that often parallel those in the cybersecurity domain. This presentation will focus on the characteristics shared among many HROs and how organizational cybersecurity efforts might improve based on those core elements.

Keywords

Cybersecurity, high-reliability organizations, dynamic non-events

EXTENDED ABSTRACT

Organizations worldwide experience negative cybersecurity incidents. Even those organizations focused on cybersecurity (e.g., LastPass) or the protection of national security are not immune. While organizations' adoption of general (e.g., NIST, CIS) and industry-specific (e.g., FERPA, GLBA, HIPAA) security/privacy standards, practices, etc. has increased, the confluence of new technologies, hybrid work environments, and ever-increasing interorganizational system integration extends organizational risk exposure and necessitates that we consider additional ways to help alleviate cyber incidents.

One domain whose findings can complement existing efforts in organizational cybersecurity is the research on high-reliability organizations (HROs) (Burns, 2019). HROs are organizations that operate in extremely hazardous conditions yet do so nearly error free for long time periods (Roberts, 1990). Nuclear submarines (Bierly III & Spender, 1995), aircraft carriers (Roberts, Rousseau, & La Porte, 1994), and utility infrastructures (Weick & Sutcliffe, 2011) are but a few examples of complex systems that function at high reliability levels despite often adverse and variable conditions.

This presentation will discuss the core elements of HROs and will link the 'dynamic non-events' found in the HRO literature (e.g., Weick, 1987) to the cybersecurity risks experienced by many modern organizations. In addition, it will explore the managerial concepts that HRO leaders utilize to foster and maintain high levels of protection motivation among employees when negative events do not occur. The overall goal is to help shed light on new ways to think about and approach organizational cybersecurity from both practical and theoretical perspectives.

REFERENCES

- Bierly III, P. E., & Spender, J.-C. (1995). Culture and high reliability organizations: The case of the nuclear submarine. *Journal of Management*, 21(4), 639-656.
- Burns, A. (2019). Security organizing: A framework for organizational information security mindfulness. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 50(4), 14-27.
- Roberts, K. H. (1990). Managing high reliability organizations. *California Management Review*, 32(4), 101-113.
- Roberts, K. H., Rousseau, D. M., & La Porte, T. R. (1994). The culture of high reliability: quantitative and qualitative assessment aboard nuclear-powered aircraft carriers. *The Journal of High Technology Management Research*, 5(1), 141-161.
- Weick, K. E. (1987). Organizational culture as a source of high reliability. *California Management Review*, 29(2), 112-127.
- Weick, K. E., & Sutcliffe, K. M. (2011). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty* (3rd ed.). Hoboken, NJ: Wiley.