Chapter 9
Equifinality in Cybersecurity Research:
Opportunities and Future Research

Brett J. L. Landry
https://orcid.org/0000-0002-0408-2408
University of Dallas, USA

Renita Murimi
University of Dallas, USA

Greg Bell
University of Dallas, USA

ABSTRACT

Cybersecurity is inherently uncertain due to the evolving threat vectors. Indeed, the constant battle between attackers and defenders in cyberspace is compounded by the multiplicity of causes, environments, threat vectors, motives, and attack outcomes. The role of improvisation and equifinality are investigated in understanding cyber incidents as incident bundles that may include both the presence and/or absence of factors that can contribute to a single outcome. Equifinality in cybersecurity operations is discussed along five dimensions: stakeholders, cyber operation bundles, end users, networks, and the threat environment for future research. For each of these dimensions, a set of themes and an associated portfolio of examples of cybersecurity activities at three levels—individual, firm, and community—is provided. Qualitative case analysis (QCA) can be employed to understand incident bundles better to understand that incidents vulnerabilities and solutions use equifinality in their paths to a given outcome.

DOI: 10.4018/978-1-6684-9018-1.ch009

INTRODUCTION

Among the many characterizations of the complex cybersecurity landscape in our environments, none is more apt than that of a high-uncertainty environment (Anant et al., 2019). The high uncertainty inherent in cyberspace is a direct outcome of the evolving threat vectors that seek to disrupt the many digital networks we inhabit. These threat vectors differ considerably in how they are manifested. For example, the failure of a particular cybersecurity control in a network supporting healthcare applications has different ramifications compared to the failure of the same control in a supply chain application. Further, the causes that lead to a cyber incident in a particular environment might be different from the causes that lead to a similar cyber incident in another environment. The same can be said about the solutions that are adopted to counter the threat vectors.

While modern cybersecurity tools are continuously evolving their mechanisms to scan the attack surface for clues about potential cyber incidents, the complexity of the networks and their attack surfaces present limitations on how we can effectively secure digital environments. For example, in the aftermath of a cyber incident, root cause analysis usually points to a set of factors that were responsible for the incident. However, the challenge posed here is that the contributing factors are only a few of the hundreds or thousands of possible points on an attack surface that threat agents could have leveraged to attack a network. Indeed, the constant battle between attackers and defenders in cyberspace is compounded by the multiplicity of causes, environments, threat vectors, motives, and attack outcomes.

The uncertainty of cyberspace has led organizations to leverage an anchor-and-adjust heuristic to mitigate the adverse effects of our bounded rationality in cybersecurity. The anchor-and-adjust heuristic, first studied in behavioral economics (Furnham & Boo, 2011), is used in situations with high uncertainty and involves choosing an anchor and then systematically moving higher or lower until any future gains in uncertainty reduction cannot be achieved with other movements. Cybersecurity measures adopted by firms over the past decades have been anchored to best practices recommended by the industry, such as the choice of solutions to protect different applications, network components, data, and systems (Tirumala et al., 2019). These solutions are then adjusted over time to reflect changes in recommendations for best practices, compliance and regulatory frameworks, threat vectors, and technology advances. For example, the NIST SP 800 (SP: special publication) guidelines on cybersecurity are provided as industry standards for best practices in various areas such as configuration, software development, vulnerability management, cryptographic key management, access controls, and dozens of other cybersecurity-related activities. These guidelines, far from prescriptive, provide recommendations for designing, developing, and maintaining secure networks and data. Their applicability to a wide range of domains and use cases makes them an apt example of an anchor, which organizations then use and adjust for their unique environments. At the same time, these guidelines offer room for improvisation or equifinality in cybersecurity operations.

The efficacy of such an anchor-and-adjust approach is rooted in the versatility of choice. Organizations can assess their own unique digital environments and evaluate their risk profile. The cybersecurity risk profile of an organization is a dynamic attribute as vulnerabilities and zero-day attacks continue to proliferate. Such a risk profile requires that organizations be equipped with a range of solutions to protect their different assets and that these solutions should be improvisable to meet their stakeholders' critical needs. One such example is the development of business continuity plans and disaster recovery plans. These plans encompass a range of threat scenarios and related recovery activities.