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.

This chapter contributes to theory and practice by introducing equifinality, a widely recognized approach in the social sciences, to cybersecurity. While this is not unfamiliar, the chapter will define and explain equifinality, configurational logic, and Qualitative Comparative Analysis (QCA). The chapter emphasizes the importance of adopting this approach into cybersecurity practice and discusses various research possibilities. Equifinality and improvisation have the potential for improving the efficiency of cybersecurity operations. Specifically, the optimal cybersecurity solution space design should be both improvisable and configurable to face the uncertainty inherent in global cybersecurity operations. The concept of equifinality, which refers to the ability to achieve a given outcome using multiple paths, is leveraged to support this argument. Specifically, a recommendation for equifinality is a significant factor in improvising and configuring cybersecurity operations.

The chapter also makes the following contributions. First, the concepts of improvisation, bricolage, and the notion that improvisation is a form of discontinuous innovation are introduced. Such a discontinuous approach to innovation in cybersecurity offers multiple ways to respond to cybersecurity threats. Next, an interdisciplinary perspective to incorporating existing research from the areas of conjunctions, equifinality, and causal complexity into cybersecurity operations is offered. With the help of cyber incident examples from three different domains (critical infrastructure, gaming, and fintech), the use of equifinality in cyber incidents is illustrated. Likewise, the chapter highlights critical research questions for future examination of analyzing cyber resilience at the individual, community, and firm levels of cybersecurity operations. Finally, the chapter gives implications for scholars and security professionals.

IMPROVISATION, BRICOLAGE, AND DISCONTINUOUS INNOVATION

The notion of improvisation crosses disciplines and domains. At a foundational level, improvisation deals with the unknown or the unplanned. The best example of improvisation is jazz music, where the musician has to play spontaneously on the spot (Barrett, 1998). Although the musicians have played the same songs with each other before, the music is dynamically changing. In a business sense, improvisation can be defined as “the ability to use time and resources to advantage in response to the unexpected and unplanned” (Meyer, 2002, p. 17).

Another term for this improvisation is the French word *bricolage*. Baker and Nelson (2005), relying on Levi-Strauss’s 1967 work, define bricolage as “making do by applying combinations of the resources at hand to new problems and opportunities (p.333).” Verjans (2005) describes Ciborra’s definition of bricolage in English as “tinkering” and suggests that this is possibly not the best definition of bricolage and offers a more common definition of ‘do-it-yourself’ as a better fit. Tinkering has a negative connotation, whereas the concept of bricolage has a positive connotation for contingency theory and improvisation. The do-it-yourself concept can be extended to situations where the problem is encountered and fixed simultaneously.

Nevertheless, there is a different lens through which to view improvisation and bricolage: innovation. Both bricolage and improvisation can be seen as discontinuous innovations rather than incremental innovations. Buffington and McCubbrey (2011) found that discontinuous innovations are developed by the creativity of experts in the area and require gaps in the existing methodologies. Whether called improvisation, bricolage, or discontinuous innovation, it is not a planned event and sometimes can only be recognized by reviewing previous activities (Fuglsang & Sørensen, 2011). The high uncertainty environments that are characteristic of cybersecurity operations require a high degree of improvisation and innovation. This is not to say that the established disaster recovery or incident response plans should be ignored or discontinued. However, it is essential to understand that the severity and scope of an incident call for multiple ways to respond to the incident.

CONJUNCTIONS, EQUIFINALITY, AND CAUSAL COMPLEXITY

Cybersecurity research has been dominated by correlational or variance theorizing, which is characterized by "the linking together of concepts expressed as dependent, independent, mediating and moderating variables, usually accompanied by formal propositions, and with a focus principally on explaining variance in outcomes" (Cloutier & Langley, 2020, pp. 1-2). However, correlational or variance theorizing is limited in its ability to develop explanations of phenomena that are marked by causal complexity (Furnari et al., 2021).

There is a growing recognition among organizational researchers that not only do many factors contribute to organizational outcomes, but they also should not be evaluated in isolation from each other. Instead, they should be examined as 'bundles,' or combinations, that may mutually enhance the ability of each to achieve critical organizational outcomes. A vital dimension of this research identifies interdependencies among multiple explanatory factors that combine to bring about an outcome of interest (Bell et al., 2014; Furnari et al., 2021). This line of research also demonstrates that understanding the simultaneous operation of multiple factors is essential for decision-makers.

Causal complexity is defined as "a situation in which a given outcome may follow from several different combinations of causal conditions" (Ragin, 2008, p. 124). This suggests that configurations are comprised of multiple explanatory factors rather than singular factors bringing about outcomes. In addition, more than one configuration could lead to the same outcome under investigation. Scholars suggest that "conjunction" focuses on how or why explanatory factors jointly bring about an outcome (Furnari et al., 2021; Mackie, 1973). Secondly, "equifinality" refers to the condition where "a system can reach the same final state, from different initial conditions and by a variety of different paths" (Katz & Kahn, 1978, p. 30).

Configurational theorizing enables researchers to transition attention from evaluations of the "net effects" of causal variables to a more contextual understanding of the multiple possible ways in which causal conditions may combine to produce a given effect (Ragin, 2008). As Iannacci and Kraus (2022) point out, configurational theorizing revolves around three tenets: 1) Conjunctural causation: the effect of a single condition unfolds in combination with other conditions; 2) Equifinality: multiple configurations (or combinations) of conditions may lead to the same outcome; 3) Causal asymmetry: the causes leading to the presence of an outcome of interest may be quite different from those leading to the absence of the outcome.

Configurational approaches are particularly appropriate when researchers argue that a combination or bundle of factors work in concert with one another to be a sufficient cause for an outcome (Mahoney & Goertz, 2006). Configurational theory provides a lens through which scholars can argue that multiple factors could produce an outcome. In addition, the theoretical lens enables scholars to argue that multiple factors can combine to lead to the outcome under investigation. This is particularly important as cybersecurity scholars increasingly recognize that outcomes under investigation are often best explained by a combination, or bundle, of factors working in concert with one another.

Fiss (2007, 2011) suggests that configurational approaches allow for the study of “multi-dimensional constellations of conceptually distinct characteristics that commonly occur together” (Fiss, 2007, p. 1180). He argues that this approach allows researchers to move beyond the singular causality and linear relationships of the linear paradigm that dominates organizational research. Instead, the configurational lens assumes a more complex and non-linear causality where factors theorized to be causally related in one configuration may be unrelated in other configurations (Fiss, 2007). In addition, this approach emphasizes the concept of equifinality, which assumes that a system can reach the same final state from various initial conditions and along a variety of paths.

Configurational theorizing benefits from thinking about linkages among the attributes combined in a configuration both in terms of the presence of specific attributes and the absence of other attributes may combine in a variety of ways to create a range of ‘recipes’ that lead to an outcome under investigation. The absence of attributes is an essential feature of configurational theorizing and points to opportunities for cybersecurity scholars. Indeed, scholars, as well as security professionals, should move beyond considering the absence of an attribute as unimportant and consider how the absence of attributes contributes to the overall impact of various bundle combinations.

While scholars are increasingly taking a configurational approach to explore organizational phenomena, much of this research has been limited to the fields of strategic management and international business (Fiss, 2007; Fiss, 2011; Furnari et al., 2021). In the following section, how equifinality can extend to cybersecurity, especially in the area of improvisation, is discussed.

DEPLOYING EQUIFINALITY FOR CYBER RESILIENCE

For organizations to succeed, they must pivot and be agile to face global opportunities and challenges. Specifically, for organizations to have agile cybersecurity operations, they must maintain an environment where it is safe to improvise (within boundaries) and go beyond established procedures. The management literature has considered equifinality due to the presence of items or activities. That is, there are many ways to achieve the same outcome, and bundles of items should be considered in reaching that outcome. Specifically, in the cybersecurity context, configurational theory enables scholars to argue that the combination of factors that lead to a cyber incident may result from the presence and the absence of different conditions or factors. Indeed, conjunctural causation is particularly useful when it is likely that there can be multiple reasons to bring about an outcome and when causal conditions could combine in unique and multiple ways to bring about an outcome.

In cybersecurity, equifinality offers the foundational construct that outcomes are the results of bundles of things, and the bundles include things that were both present and absent. To begin, there needs to be a precise definition of a cyber incident. NIST defines an incident as “an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies” (National Institute of Standards and Technology, 2006, p. 7). A common method for determining the causes of incidents is root cause analysis (RCA). However, sometimes the bundles of events contain too many possibilities to fit cleanly into an RCA. Moreover, just because an outcome was reached by one path does not mean it is the only path to that outcome.

Conger and Landry (2009) encountered this phenomenon while conducting an action-based research project with a global logistics company in the United Kingdom. The client's leadership team was convinced that their problems were due to technology, not a result of their people and processes. The researchers found that the traditional analysis tools of Ishikawa diagrams, maturity models, RCA, and 2x2 matrices did not address the client's needs due to the immaturity of IT infrastructure. The reality was that most problems were based on people and processes, not directly on technology. The researchers took an improvisation approach, understanding that the tools in their toolbox did not fit and that there were more complicated relationships at work causing the issues. The firm's low IT maturity significantly contributed to its high-entropy network. The researchers developed a new model for the client that captured the relationships and presented the items in a new way.

To illustrate how equifinality is pervasive in cybersecurity operations, cybersecurity incidents from diverse domains will be examined. The first three cases involve financial incentives for threat actors with ransomware at Colonial Pipeline, theft of intellectual property at EA Games, and identity theft and extortion at Robinhood. The fourth case at the Oldsmar water treatment plant highlights the fragility of digitized critical infrastructure, where the threat actor intended to harm the public.

Colonial Pipeline

Consider the May 2021 Colonial Pipeline ransomware attack that led to a six-day production outage (U. S. Department of Energy, 2021). While there are a variety of bundles of ways to perform this attack, there was a specific bundle of activities that took place. First, a Colonial Pipeline VPN password was used on another system that had been compromised (Culafi, 2021). It is unknown what system was compromised, but the password was part of a group found on the dark web (Fung & Sands, 2021). Once inside the network, the threat actor stole 100 gigabytes of data and encrypted Colonial's internal IT systems using ransomware as a service software (Kerner, 2022). It was reported that the ransomware did not impact their operational technologies (OT) because Colonial quickly shut down the enterprise systems.

These activities can be included in an incident bundle. First, password reuse is the mechanism through which threat actors entered the network via the VPN. Secondly, it was wrongly assumed that this legacy account profile was not active on the VPN but in fact, was still active. Thirdly, the legacy VPN account did not require multi-factor authentication (MFA) (Kelly & Resnick-ault, 2021). Fourth, while VPNs are designed to protect crucial network resources from threat actors, it allowed direct encrypted access into the Colonial network in this case. Fifth, although the compromised password used complexity in both length and special characters, this measure failed to stop the attack because the password was already breached and used on multiple systems. Lastly, although Colonial Pipeline invested over $200 million in IT systems during the previous five years (Kelly & Resnick-ault, 2021), this investment did not block the attack.

The incident bundle for Colonial Pipeline is included in Table 1. It is important to note that viewing this cyber incident through the lens of equifinality is one way to analyze the causes of this incident, but it is not the only way. The variability of attack methods and tools is the biggest challenge for cyber defenders. The defenders must get it right every time; the threat actors only need to get it right once.

Table 1. Colonial pipeline incident bundle

Item	Issue
Reused password	• Once one system is compromised, all systems are compromised that use shared passwords
Passwords breached and leaked to the dark web	• Password breach may be unknown • If known, passwords should be changed
Legacy VPN account	• VPN is an open door into the network
VPN authentication	• VPN used SFA only. If MFA had been employed, the incident could have been prevented
Password complexity	• Password complexity does not stop compromised password usage
$200 million IT investment	• IT investment did not prevent the incident

EA Games

Similar to how cybersecurity defense employs equifinality, threat actors also improvise and employ equifinality in their approaches to attack networks and systems. The EA cyber incident is an excellent example of how equifinality was employed by both the attackers and defenders. Threat actors were able to steal 780 GB of data from the EA Games network. Stolen session cookies were bought on the dark web for $10 to gain access to the firm's Slack channel (Fung, 2021; Spadafora, 2021). With a small amount of social engineering, the threat actor was able to use Slack to message and convince IT to send them an MFA token. This allowed the threat actor to bypass MFA controls and successfully enter the network. The threat actor then built persistence into the network and created a virtual machine to explore the network and exfiltrate 780 GB of data, including source code, software development kits, and proprietary tools. The EA Games incident bundle is discussed in Table 2.

Table 2. EA Games incident bundle

Item	Issue
Stolen session cookies	• A threat actor masqueraded as a valid user to connect to Slack
Social engineering	• IT was tricked into issuing a MFA token to the threat actor based on a Slack connection
Network persistence	• A threat actor was able to build a stable connection to enumerate the network
Rogue virtual machine	• A threat actor was able to build a platform to exfiltrate data

Robinhood

If a threat actor wanted to get into an enterprise network, why not just ask for remote access? In November of 2021, Robinhood, a stock trading app, reported a data breach on approximately seven million customer accounts (Brown, 2021; O'Brien, 2021). Robinhood stated that a threat actor was able to social engineer a customer support employee over the telephone to install remote access software on his PC (Abrams, 2021; Barry, 2021). The threat actor then attempted to extort Robinhood for money (Egan, 2021). Robinhood said they contacted law enforcement when asked to pay the extortion fee. A few days after the attack, the threat actor was selling the data on hacking forums (Abrams, 2021). As a result, approximately 40,000 Robinhood customer accounts have been victims of cyber-attacks after the original breach (Avery, 2022). The Robinhood incident bundle is discussed in Table 3.

Table 3. Robinhood incident bundle

Item	Issue
Social engineering	• IT staff member was tricked into installing remote access software
Network persistence	• A threat actor was able to build a stable connection to enumerate the network

Oldsmar Water Treatment Plant

The Oldsmar water treatment plant in Florida was hacked in February 2021 due to a collection of problems. First, the targeted computer was running Microsoft Windows 7, which is no longer supported. Second, this PC allowed remote access with a program called TeamViewer with a password that was shared among users and used on all computers at the plant. Third, the PC was directly connected to the Internet without a firewall (Matthews, 2021). The attack was discovered when an operator noticed the mouse cursor moving independently (Bergal, 2021). By gaining remote access to the PC controlling the water chemicals, the threat actor increased the sodium hydroxide (lye) level in the water supply to 100 times the standard amount. The action was reversed before harm could be done.

In this case, there were several vulnerabilities: an old operating system, shared passwords among users, shared passwords among PCs, single-factor authentication, and the lack of a firewall. However, only two of these items contributed to the incident bundle, the shared passwords among users and PCs and single-factor authentication, as shown in Table 4. The end-of-life Windows 7 computer is a vulnerability for the operating system and, most likely, the hardware. The incident could have occurred on a Windows 11, a Mac, or a Linux device if they had remote access software installed with a shared password. The lack of a firewall is a definite concern, but like the operating system, it did not directly contribute to this incident bundle. If remote access was needed to this PC, then there would be firewall exceptions to allow connectivity. So, the legacy PC and the lack of a firewall are components of an alternative incident bundle, as shown in Table 5.

Table 4. Oldsmar Water Treatment Plant incident bundle

Item	Issue
Shared passwords among users and machines	• Easy-to-use password scheme • One password allows access for everyone and everywhere
Single-factor authentication for remote access	• Password is the only factor used

Table 5. Alternate hypothetical Oldsmar Water Treatment Plant incident bundle

Item	Issue
Windows 7 Computer	● Legacy hardware and operating systems ● Lack of hardware refresh cycles ● Possible legacy software/hardware compatibility issues
No firewall	● A firewall did not protect the PC

Deploying Incident Bundles and Equifinality

This list of data breaches illustrates how incident bundles and equifinality can play a role for the threat actor to compromise cyber targets. Additionally, for each of these incidents mentioned, many alternate attack methods and tools could be used and exploited. Cyber defenders can use equifinality in their network monitoring and change the existing mindset in cybersecurity to emphasize that cybersecurity is everyone's job. This could be something as simple as deploying honeypots on every subnet to generate early warnings of network reconnaissance (Landry & Koger, 2023b).

Defense in depth, while widely studied and implemented, has been a protection strategy that has not adequately protected networks and data repositories. As a result, organizations should transition towards zero trust network architectures (ZTNA). ZTNA is not a technology but a new way to examine protection using security by design (Landry & Koger, 2023a). ZTNA requires an understanding of every device on the network and understanding how it could be used for both good and bad activities. This dual purpose of devices fits well into equifinality and bundles in cybersecurity operations. For example, while a legacy device can provide a connection to historical data, the same legacy infrastructure can also be used by threat actors to launch attacks across the network. So, if the organization had a legitimate need for a Windows 7 computer, the configuration bundle would need other protection mechanisms, such as external firewalls or isolation from the network. It is the combination of these items that creates the security bundle for the Windows 7 computer.

Newer technologies such as cloud computing, infrastructure as code, blockchain, and IoT must also be considered in a security bundle before a breach or in an incident bundle post-event. A primary consideration is that poor network architecture, weak access controls, and undocumented processes are absolute problems in an on-premise environment. Migrating these problems to hybrid or full cloud implementations does not fix the issue; it only transfers where the problem is located. It does, however, change the incident bundle with new and different concerns than when these items were on premise.

DIRECTIONS FOR FUTURE RESEARCH

There are many opportunities for research investigating equifinality and configurations in cybersecurity. Below, the focus of the discussion of equifinality in cybersecurity operations is expanded along five dimensions: stakeholders, cyber operation bundles, end users, networks, and the threat environment (see Table 6 for a summary of these dimensions). 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. The individual level comprises cyber-related decisions and activities that people perform when dealing with systems, networks, and data. A top-down approach to designing and implementing cybersecurity policies and controls characterizes firm-level decisions and activities. An example of a firm-level set of actions would be adopting a specific firewall or migrating to a cloud service provider.

On the other hand, the community level encompasses a grassroots, bottom-up approach to decision-making, exemplified by open-source communities, hacker communities, and even the communities that make up our living and working environments. The concerns of each of these entities (individual, firm, community) differ regarding cybersecurity, and so do their approaches toward adopting bundles that achieve equifinality in cybersecurity operations. Each of these dimensions are discussed in detail below.

Stakeholders

The concept of motives, opportunities, and means (Grabosky, 2001) has been used widely in cybersecurity literature as a way to analyze the growing trend of cybercrime. The same concept of motives, opportunities, and means to analyze how individuals, firms, and communities can adopt equifinality in configuring their cybersecurity solution space. Consider the role of stakeholder motives, which can be leveraged to maximize the effectiveness of an equifinal configuration of cybersecurity solutions. At the individual level, consider a user who is unable to login into their work account for a brief period of time. In an attempt to maximize efficiency, the user emails work files to their personal email account and works on those files despite the lack of access to the work account. The motives for this lapse are undoubtedly justified, and the work still gets completed, but there is a lapse in the network perimeter.

At the firm level, organizations are equipped with different sets of resources, which provides them with an unequal footing to maintain and improve the security of their systems and networks. Organizations that lack in-house cybersecurity expertise and resources use managed security service providers (MSSP) or cloud solutions services, thus obtaining external resources for equifinal cybersecurity solutions. At the community level, consider an open-source software code community that uses code reviews, bug bounties, hackathons, and other mechanisms to improve the efficiency of the codebase in a distributed manner. In each of these cases, the motives for adopting cybersecurity solutions differ, thus leading to the equifinality of cybersecurity operations.

Table 6. Directions for future research

Critical Research Questions for Future Study	Individual Level	firm Level	Community level
Stakeholder (motives-opportunity-means)			
How can stakeholders' motives be leveraged to maximize the effectiveness of an equifinal configuration of cybersecurity solutions?	How can we create solutions for users to avoid sending work data to a personal account?	How can organizations that lack in-house cybersecurity resources use external services for equifinal cybersecurity solutions?	How can open-source communities that use code reviews, bug bounties, and hackathons to improve the efficiency of the codebase in a distributed manner?
How can stakeholders use desire path opportunities to improve, rather than, hinder the effectiveness of cybersecurity solutions?	How can users refrain from password sharing with an understanding why a certain password policy dictates frequent change, complexity, and uniqueness?	How could firm-level restructuring present opportunities for desire paths?	How can we increase the understanding of the relationship between good cybersecurity posture and cyber resilience?
How can stakeholders efficiently indicate their commitment and adoption of equifinal approaches to cybersecurity without oversharing or under-sharing?	How can users be encouraged to be mindful of data-sharing to limit potential malicious OSINT/HUMINT activities?	How can firms use phishing campaigns to identify the baseline of phishing awareness and improve these baselines?	How can community discovery of bug bounty programs be used prudently to improve cybersecurity posture?
Bundle (bundle overload – dynamicity – sociotechnical perspectives)			
How does the dynamicity of cybersecurity solutions affect the ability to create equifinal paths?	How can we simplify the credential management process for users, who are typically faced with multiple accounts?	How can organizations make informed decisions about changes to their network architecture to avoid crucial components from going offline for extended periods?	How can communities manage equifinal cybersecurity operations with an understanding that the culture informs the technology design and implementation?
For a given equifinal configuration, what is the process of updating individual paths and discovering their impact on other paths?	How can users make informed decisions about equifinality in secure operations for everyday computing and connectivity?	How might organizations benefit from the expertise and vision of boards with cybersecurity-minded individuals?	How does a smart city's equifinal cyber configuration differ from that of a rural community?
How do the attributes of a bundle impact the efficiency of the equifinal configuration?	Is there a tipping point beyond which usability concerns override security concerns among users?	How is the valuation of companies impacted in the wake of cyber incidents?	How are the social dynamics of communities factored into the development of information-sharing platforms?
End-user (biases – limitations – strengths)			
How can end users recognize their limitations in navigating equifinal cybersecurity outcomes?	How can we nudge users toward voluntary adoption of best practices in equifinal cybersecurity operations?	How can firms move toward adopting a holistic approach to cybersecurity?	How can communities rely on the security of technologies that power these environments?
How can firms create cybersecurity solutions that are mindful of users' biases while still navigating equifinality in solutions?	How can users entrust the security of their accounts to the service providers?	How can companies build risk profiles considering biases that affect the adoption of equifinality in cybersecurity operations?	How can collective biases which lead to collective circumvention of security controls be avoided?
How can the cognitive strengths of users be leveraged alongside emerging technologies to create adaptable solutions spaces?	How can our multiple intelligences be leveraged alongside the narrow intelligence of AI-enabled tools for cybersecurity operations?	How can firms' choice of security controls be informed by equifinality?	How can communities bundle cyber security technologies for their needs?
Network (centrality – assortativity – tie strengths)			

Continued on following page

Table 6. Continued

Critical Research Questions for Future Study	Individual Level	firm Level	Community level
How does the centrality of nodes impact the decisions about equifinality in cybersecurity operations?	How do people share information about their security controls of choice?	How do highly competitive environments cause firms to sacrifice security in favor of agility?	How do communities determine the elements of critical infrastructure that are central to their functioning?
How do the assortativity tendencies in security control adoption impact the decisions about equifinality in cybersecurity operations?	How do users overestimate their tendencies to be security-conscious and underestimate their proneness to breaches?	How do failures of security controls lead to lawsuits and personnel termination at firms?	How does vendor monopoly and herd mentality cause similar security controls to be used throughout an industry vertical?
How might adoption of security controls (nodes) in well-resourced environments differ from those in low-resourced environments?	How efficient are users' mental models in the understanding the complexity of the networks they inhabit?	How can we create equifinality in cybersecurity operations for differently-resourced environments?	How do communities respond to the pressure to consider investment in equifinal cybersecurity controls?
Environment (Threat landscape – technology complexity - regulation)			
How do perceptions of the cybersecurity threat landscape vary?	Do individuals adopt mostly free technologies, ignore threats, or respond with the minimum possible effort?	Do organizations participate in knowledge sharing initiatives such as cves to disseminate information?	Do communities provide forums for regular inventory of security controls of critical infrastructure?
How does the black-box-like nature of emerging technologies like AI, ML, blockchain, and IoT impact equifinality of cybersecurity operations?	What factors cause individuals to rush to adopt newer technologies without fully understanding security implications?	How does cyber insurance fit into an equifinal bundle for cybersecurity operations?	What factors cause communities to ban certain technologies?
How is the regulatory landscape affected by the environment?	How do users understand the implications of violating the terms of use in their varied computing and networked environments?	How do firms' actions protect or render it liable to unprecedented legal rulings?	How can equifinality of IoT operations help communities mitigate disastrous outcomes from IoT compromise?

A similar case can be made for opportunities that leverage instead of attempting to eliminate desire paths. Desire paths, commonly used in architecture, refer to people's shortcuts to navigate the physical space around them (Smith & Walters, 2018). For example, people would rather trample upon grass instead of taking the longer paved path to quickly reach a particular building entrance. Similar instances can be found in cybersecurity behaviors such as shadow IT. While desire paths in architecture, human-computer interaction, or cybersecurity cannot be eliminated, they can be leveraged to rethink the design of a bundle of equifinal cybersecurity operations. At the individual level, consider the problem of a password policy that dictates frequent change, complexity, and uniqueness to encourage users to refrain from password sharing across sites and accounts, which represents a desire path (Singer et al., 2013). Firms that undergo restructuring due to internal or external factors also present a prime opportunity for employees and administration to take desire paths instead of dealing with the challenges of developing secure networks (Lohrke et al., 2016). At the community level, consider a rapidly changing set of critical infrastructure components that are being connected to cloud services via the Internet. This increases convenience, efficiency, and ease of access but also presents a large attack surface (Foreman & Gurugubelli, 2015). Communities should be mindful of the desired path in rapid digitization and find ways to improve their cybersecurity and cyber resilience.

How equifinality in cybersecurity operations is achieved is equally important. The structure of a stakeholder's bundle of equifinal cyber solutions may or may not be as helpful in informing the structure of another's stakeholder's equifinal bundle. Sharing resources or information about resources is helpful but also expands the attack surface. For example, given the wide variety of social networking platforms for work and leisure, individuals need to be mindful about how much data they share in limiting potential malicious open-source intelligence/human intelligence activities that could correlate between databases and extract crucial inferences (Kelleher et al., 2020). An organization's findings about the baseline of phishing awareness can be used positively or negatively by external stakeholders. Similarly, communities of independent stakeholders, such as those who participate in bug bounty programs, may discover items of varying importance to the cybersecurity posture, and companies need to be prudent in managing the scope of discovered bugs by third parties (Kuehn & Mueller, 2014).

Bundles of Solutions

The bundle of solutions adopted to address cybersecurity challenges varies according to the needs being met. Due to the rapidly changing nature of technologies and the threat environment, bundles are not static and must be frequently revisited to update the bundle's components. While having a choice of potential solutions to incorporate in a bundle is helpful, this bundle overload also leads to decision fatigue when it comes to adoption. This is especially true due to the dynamic nature of the solutions and the need to adapt these bundles to meet the needs of communities in their distinct environments. Directions regarding the bundle in terms of its dynamicity, attributes, and codependencies between bundle elements that affect the design and implementation of equifinal bundles for cybersecurity operations are provided here.

The dynamicity of bundles impacts individuals, firms, and communities differently. For example, at the individual level, users are faced with a plethora of login credential requirements for different accounts and find it challenging to keep up with account change and management. Here, a bundle of login credentials for access to different kinds of accounts makes it challenging for users to find services for credential management. Similarly, due to the highly embedded nature of technology within every industry vertical, organizations must make informed decisions about changes to their network architecture to avoid crucial components from going offline for extended periods. Finally, within communities, the adoption of certain kinds of technology for a given need does not translate to equivalent performance or security guarantees. For example, the choice of a water utility online bill pay system for a community of 50,000 people differs from that of a rural community using residential water sources (Malecki, 2003).

Bundles are also inherently dynamic. For example, the botnets that were heavily leveraged to spread spam have now found utility in ransomware command and control operations (Jarjoui et al., 2021; Murimi, 2020). Since threats constantly evolve, a bundle's individual elements must be updated, replaced, or modified. Entities must find resources for updating individual paths and discovering their impact on other paths. One such instance is users' decisions regarding products for everyday computing and connectivity usage. Organizations face such decision-making challenges on a much larger scale, such as choosing individuals to serve on the boards. While in the past, boards have traditionally been comprised of individuals representing essential business functions; it is becoming increasingly important for boards to have representation of cybersecurity-minded individuals (Rothrock et al., 2018). At the community level, digital connectivity defines the adoption of many technology-dependent solutions (Salemink et al., 2017).

As illustrated earlier in this chapter, a cyber incident may have different causes in different environments. Consequently, the incident bundles need adaptable solution bundles, which also define the concept of equifinality in cybersecurity operations. The attributes of a bundle, as measured by the types of resources in the bundles, the challenges that these resources are designed to meet, and the significance of each of these resources for other elements in the bundle and for the entire bundle itself, impact the efficiency of the equifinal configuration. For individual users, there exists a tipping point beyond which users will value usability more than security (Nurse et al., 2011). The same is also true for privacy, where users will adopt technology, especially newer IoT technologies such as voice-based assistants, because of usability and not because of the security controls provided (Awojobi & Landry, 2023).

Regarding this discussion on equifinal bundles of solutions, beyond the tipping point, solutions prioritizing usability will be weighted higher than those focusing on security. Furthermore, regulation and compliance, along with the power of social media, have created complex post-breach environments that can have lasting consequences for both the organization and the affected individuals. Finally, the social dynamics of communities also factor heavily in how information is exchanged on social media platforms, which have turned into veritable information-sharing platforms (Cyr & Wei Choo, 2010).

End-User

End users have been famously, but not always accurately, portrayed as the weakest link in our networks. Our cognitive biases and limitations in understanding the scope and granularity of the complex networks that we inhabit inform the ways in which we interact with computing technology (Caraban et al., 2019). The equifinality of solutions for cybersecurity operations is one of the mechanisms in which our biases and limitations can be viewed as strengths in terms of choosing solutions that best address our security needs in the digital space.

The limitations of end users affect our personal, professional, and social lives. Like the nudging mechanisms enabling responsible stewardship, such as double-sided printing the default (Thaler, 2018), users can also be nudged toward default security operations (Acquisti et al., 2017). Within organizations, cybersecurity has traditionally been the purview of the IT departments. However, this approach is flawed since it causes cybersecurity to be approached as a siloed business function. In contrast, cybersecurity is best addressed when firms move forward, adopting a holistic approach to cybersecurity by integrating it into business functions across the community (Jarjoui & Murimi, 2021). At the community level, the efficient operation of our everyday work, home, and leisure environments is dependent on the security of technologies that power these environments, making it all the more imperative to be mindful of our limited understanding of the security of these technologies.

Kahneman and Tversky (2012) famously refuted the notion of the rational human and showed how heuristics and biases govern our decision-making processes. Knowing that our biases inform our interactions with our computing environments, individuals cannot be lax in entrusting the security of their accounts to the companies that provide services. Organizations, too, must build risk profiles with an understanding of their data and system assets, which will aid in understanding how biases affect the adoption of equifinality in cybersecurity operations. Existing literature abounds in identifying how the wisdom of the crowds sometimes is not really wisdom, but conformity to social thought, even if it is flawed (Lorenz et al., 2011). Thus, collective decision-making suffers from the amplification of individual biases due to pressures of the herd mentality (Loxton et al., 2020), leading to collective circumvention of security controls, and communities have to be mindful of these biases when adopting equifinal bundles of security solutions (Wu et al., 2022).

However, despite biases and limitations, leveraging multiple intelligences and rapidly adapting to new circumstances confers a unique advantage. A recent wave of generative predictive AI tools have shown that these tools, while intelligent, are still only good at one or a few tasks (Fox, 2017). When aided by these tools, our cognitive strengths offer individuals, firms, and companies a wide range of possibilities in achieving equifinality in cybersecurity operations as well.

Network

Graph-theoretic models of networks have been used extensively in uncovering patterns of flows within networks. This section examines applications of network effects (centrality, assortativity, and tie strengths) to cybersecurity solutions by considering the nodes in a network as security controls and the edges between nodes as codependencies between security controls. By notating security controls and their codependencies in this manner, network science offers tools to uncover the most influential nodes in a network, the most valuable links between nodes, and uncover patterns of clustering. One such pattern is denoted as assortativity, which refers to the rich-get-richer effect, also known as the Matthew effect, where nodes with more extensive networks keep getting larger (Cheng et al., 2019). Another pattern is centrality, which denotes the importance of a node in information flows through the network. In our context, a node with a high centrality index indicates a widely adopted solution. Similarly, tie strengths, first studied by Granovetter (1973) to describe strong and weak social ties in human networks, can be used to analyze the codependency links between security solutions in an equifinal approach to cyber solutions.

From the perspective of security controls as nodes in a network that represents the cybersecurity operations spaces, it is interesting to analyze how the centrality of nodes impacts the decisions about equifinality in cybersecurity operations. At the individual level, users share information about their cyber solutions, such as the choice of a password vault application or anti-virus software, with their family, friends, and acquaintances. This word-of-mouth endorsement creates conditions that enable the adoption of certain controls more than others. A similar effect can be found in organizations, where word-of-mouth information about the activities of peer and rival firms in competitive environments causes firms to adopt similar cybersecurity processes, which may result in a tradeoff between security and agility of product launches (Winterrose et al., 2016). Communities, too, are prone to such behavior where similar cyber solutions are adopted due to their usage in similar communities (Arce, 2020). While these approaches might signal the efficiency of a particular solution, they also hinder the consideration of equifinality in cyber operation solutions as individuals, firms, and communities fail to consider their own distinct cybersecurity environments.

This reluctance or inability to consider equifinal operations that are customized for one's own needs results in assortativity in terms of solution adoption. This is true for individual users in networks, who have been shown to overestimate their tendencies to be security-conscious and underestimate their proneness to breaches. At the firm level, the tendency toward assortativity of solution adoption might lead to cyber incidents, leaving companies with lawsuits and the termination of key employees. The herd mentality similarly causes vendor monopoly and the adoption of similar security controls to be used throughout multiple industry domains.

Individuals, firms, and communities are endowed with different kinds of resources for cybersecurity, where some entities possess disproportionate levels of resources in dealing with cyber threats compared to others. This gives such well-resourced entities an upper hand in managing and responding to cyber incidents. It is important to note that equifinality presents a promising option to deal with this problem since organizations and communities can adopt solution bundles that fit their needs. This is helpful for individual users, who rarely understand the complexity of the networks they inhabit and instead rely on mental models to guide their decisions regarding bundle formation (Brase et al., 2017).

Environment (Threat Landscape – Technology Complexity – Regulation)

The environment within which cybersecurity operates is constantly under change. This change comes from three broad factors – the changing threat landscape, the increasing complexity of existing and emerging technologies, and the evolving regulatory domain. Newer forms of malware, applications, and regulatory requirements present unique challenges in cybersecurity operations, and equifinality is poised to be an efficient mechanism for dealing with the environmental challenges posed by these three factors.

Individuals, firms, and communities are faced with a multitude of options, ranging from free to freemium and paid subscription models, to manage their cybersecurity solutions. At the individual level, it is interesting to analyze the factors that contribute to people's decisions to choose a particular cybersecurity solution. These factors could be the cost, ease of access and usage, popularity, or other behavioral factors (Pfleeger & Caputo, 2012). At the firm level, the vast array of available options and the lack of information about the vulnerabilities in these options has given rise to several knowledge-sharing platforms, such as the Common Vulnerability Enumeration (CVE) list, which serves as a dynamic catalog of vulnerabilities in platforms and applications. First proposed by MITRE and now managed by a partnership of industry, academic, and government institutions, the CVE is a widely used platform for gaining information about vulnerabilities (MITRE Corporation, 2023). The CVE is also community-led, and its success depends on the participation of organizations in reporting and disseminating information about vulnerabilities. Open-source and bug bounty communities have similarly responded with community-led initiatives for information sharing about vulnerabilities and flaws, creating an ecosystem of flaw discovery and remediation (Ponta et al., 2019).

With newer technologies, the attack surface increases because of the tendency toward abstraction. The rise of applications powered by artificial intelligence (AI) and machine learning, as well as the demands of newer technologies such as blockchain and Internet of Things, all pose massive demands on our networks and our cognitive capacity for understanding the operation, complexity, and implications for our everyday life. As individuals rush to adopt newer technologies, such as mining of cryptocurrencies, using generative predictive AI tools, and adopting smart home technologies without fully understanding security implications, the attack surface rises proportionately (Ayinala & Murimi, 2022; Bécue et al., 2021; Edu et al., 2020; He et al., 2020; Saad et al., 2020). Firms have responded to this crisis in various ways, including using cyber insurance to protect against the unintended outcomes of cyber incidents (Marotta et al., 2017). Similarly, the decision of specific communities to ban applications of certain technologies represents another mechanism to deal with the uncertainty of the adoption of new technologies (Conger, K. et al., 2019; Gadzheva, 2007; Meckling & Nahm, 2019; Taylor, 2016). Such decisions, although myopic, serve to provide stopgap solutions while other solutions of deeper scope are being formulated.

Governments and institutions have attempted to regulate various aspects of technology, but the gap between law and technology is increasing faster with the strides in technology advances. This has significantly affected the regulatory landscape. For example, individuals routinely use work computers to conduct personal activities while unaware of the scope of the terms of use (D'Arcy et al., 2014). At the organizational level, companies have to rethink their technologies' broader implications, as seen in the Gonzalez v Google case (2023). In this case, the Gonzalez family brought a lawsuit against Google accusing its YouTube recommender algorithms of providing training for jihadist organizations such as ISIS, whose Paris attack was responsible for the death of Nohemi Gonzalez. At the community level, the equifinality of IoT cybersecurity operations must also be considered with a granular lens since IoT compromises can result in disastrous outcomes (Kimani et al., 2019).

DISCUSSION

Cybersecurity scholars and security professionals should look to methodologies geared to understanding configurations that lead to incidences as well as those associated with recoveries. One worthwhile methodology is Qualitative Comparative Analysis (QCA) which is grounded in a set-theoretic approach that develops causal claims utilizing supersets and subsets (Ragin, 2008). QCA is especially helpful because the methodology allows for an outcome to be produced by multiple conditions. In addition, the methodology helps to identify how multiple factors can combine to lead to the outcome under investigation. Finally, QCA allows for outcomes to occur due to either the presence of variables or their absence. The number of scholars investigating economic and organizational phenomena with set-theoretic methods has risen considerably in the last few years (Fiss, 2007; Fiss, 2011; Grandori & Furnari, 2008; Pajunen, 2008).

QCA's approach to causality, referred to as multiple conjunctural causation, has three important implications. First, an outcome can be produced by multiple conditions. Second, QCA recognizes that multiple conditions can lead to the outcome under investigation. This is known as equifinality, and it is a central element of QCA. Third, QCA allows for outcomes to occur as a result of the presence or absence of a condition. Conjunctural causation is particularly useful when it is likely that there can be multiple reasons to bring about an outcome and when causal conditions could combine in unique and multiple ways to bring about an outcome. The methodology is not centered on variable distributions and the search for patterns of covariation, difference, or frequency clustering.

Moreover, QCA relaxes some of the assumptions often associated with quantitative techniques, such as permanent causality, additivity, and causal symmetry (Ragin, 2008). Instead, the technique is quite helpful in evaluating both the number and complexity of alternative paths leading to a desired outcome. QCA can be deployed in investigating cyber incident bundles using either crisp (binary membership) or fuzzy (membership percentages) sets to explore multiple cases at the same time to example what factors were present, absent, or did not contribute.

Implications for Educators

Educators need to create scenarios that develop and reinforce the concepts of equifinality, improvisation, and bricolage. This goes beyond examining previous breaches where the causes can be obtained through an online search. Such a scenario-focused analysis involves developing Kobayashi Maru scenarios where learners are presented with the choice between two options, both of which are bad decisions (Stemwedel, 2015). Learners can then choose one of the bad decisions or use the new tools to develop an entirely new solution. It involves reframing the problem and understanding which constraints are fixed and which ones are variable and can be changed to develop new solutions.

Implications for Security Professionals

The cyber landscape is not going to flatten or get simpler. The number of critical vulnerabilities, data breaches, ransomware, and attacks not conceived yet will only continue to increase. With every asset, every protection mechanism, and every vulnerability, security professionals should take the equifinality approach and consider them in related bundles and not in isolation. There are various ways to make this change, from isolated items and events to related bundles. The first is brainstorming and tabletop exercises so that more people are involved in developing solutions providing a difference in thought as well as abilities. Participants can then examine and explore multiple alternative paths for every process, solution, or threat using improvisation for totally new solutions. During this examination, it is essential to focus not only on policy and procedures but on the desire paths of how processes are actually done. Finally, it is critical to examine solutions from different stakeholder levels (individual, firm, community). By employing equifinality and improvisation, security professionals can be more agile and better prepared for the threats around the corner.

REFERENCES

Abrams, L. (2021). *7 million Robinhood user email addresses for sale on hacker forum.* BleepingComputer. Retrieved on June 2, 2022, from: https://www.bleepingcomputer.com/news/security/7-million-robinhood-user-email-addresses-for-sale-on-hacker-forum/

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L., Komanduri, S., Leon, P., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for privacy and security. *ACM Computing Surveys*, *50*(3), 1–41. doi:10.1145/3054926

Anant, V., Bailey, T., Cracknell, R., Kaplan, J., & Schwartz, A. (2019). *Understanding the uncertainties of cybersecurity: Questions for chief information-security officers.* McKinsey & Company. Retrieved on September 4, 2022, from: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-blog/understanding-the-uncertainties-of-cybersecurity-questions-for-chief-information-security-officers

Arce, D. G. (2020). Cybersecurity and platform competition in the cloud. *Computers & Security*, *93*, 1–9. doi:10.1016/j.cose.2020.101774

Avery, D. (2022). *Robinhood app's $20 million data breach settlement: Who is eligible for money?* CNET. Retrieved on October 19, 2022, from: https://www.cnet.com/personal-finance/banking/robinhood-20-million-settlement-who-is-eligible-for-money/

Awojobi, B., & Landry, B. J. L. (2023). An examination of factors determining user privacy perceptions of voice-based assistants. *International Journal of Management*, *Knowledge and Learning*, *12*, 53–62. doi:10.53615/2232-5697.12.53-62

Ayinala, S., & Murimi, R. (2022). On a territorial notion of a smart home. In *Proceedings of the 1st Workshop on Cybersecurity and Social Sciences* (pp. 33–37). Association for Computing Machinery. 10.1145/3494108.3522766

Baker, T., & Nelson, R. E. (2005). Creating something from nothing: Resource construction through entrepreneurial bricolage. *Administrative Science Quarterly*, *50*(3), 329–366. doi:10.2189/asqu.2005.50.3.329

Barrett, F. J. (1998). Creativity and improvisation in jazz and organizations: Implications for organizational learning. *Organization Science*, *9*(5), 605–622. doi:10.1287/orsc.9.5.605

Barry, C. (2021). *Robinhood breach illustrates the impact of social engineering attacks.* Retrieved on March 22, 2022, from: https://blog.barracuda.com/2021/11/19/robinhood-breach-illustrates-the-impact-of-social-engineering-attacks/

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), 3849–3886. doi:10.100710462-020-09942-2

Bell, R. G., Filatotchev, I., & Aguilera, R. V. (2014). Corporate governance and investors' perceptions of foreign IPO value: An institutional perspective. *Academy of Management Journal*, *57*(1), 301–320. doi:10.5465/amj.2011.0146

Bergal, J. (2021). *Florida hack exposes danger to water systems.* https://pew.org/3btxWBc

Brase, G. L., Vasserman, E. Y., & Hsu, W. (2017). Do different mental models influence cybersecurity behavior? Evaluations via statistical reasoning performance. *Frontiers in Psychology*, *8*, 1929. doi:10.3389/fpsyg.2017.01929 PMID:29163304

Brown, S. (2021). *Robinhood data breach is bad, but we've seen much worse.* CNET. Retrieved on June 2, 2022, from: https://www.cnet.com/news/privacy/robinhood-data-breach-is-bad-but-weve-seen-much-worse/

Buffington, J., & McCubbrey, D. (2011). A conceptual framework of generative customization as an approach to product innovation and fulfillment. *European Journal of Innovation Management*, *14*(3), 388–403. doi:10.1108/14601061111148852

Caraban, A., Karapanos, E., Gonçalves, D., & Campos, P. (2019). 23 ways to nudge. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-15). https://doi.org/10.1145/3290605.3300733

Cheng, C., Wang, H., Sigerson, L., & Chau, C. (2019). Do the socially rich get richer? A nuanced perspective on social network site use and online social capital accrual. *Psychological Bulletin*, *145*(7), 734–764. doi:10.1037/bul0000198 PMID:31094537

Cloutier, C., & Langley, A. (2020). What makes a process theoretical contribution? *Organization Theory*, *1*(1), 1–32. doi:10.1177/2631787720902473

Conger, F. R., & Kovaleski, S. F. (2019, May 14,). San Francisco bans facial recognition technology. *The New York Times.* https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Conger, S., & Landry, B. J. L. (2009). Problem analysis: When established techniques don't work. In *Proceedings of the Conf-IRM Conference* (pp. 1-8). Academic Press.

Culafi, A. (2021). *Mandiant: Compromised Colonial Pipeline password was reused.* Retrieved on July 14, 2022, from: https://www.techtarget.com/searchsecurity/news/252502216/Mandiant-Compromised-Colonial-Pipeline-password-was-reused

Cyr, S., & Wei Choo, C. (2010). The individual and social dynamics of knowledge sharing: An exploratory study. *The Journal of Documentation*, *66*(6), 824–846. doi:10.1108/00220411011087832

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285–318. doi:10.2753/MIS0742-1222310210

Edu, J. S., Such, J. M., & Suarez-Tangil, G. (2020). Smart home personal assistants. *ACM Computing Surveys*, *53*(6), 1–36. doi:10.1145/3412383

Egan, M. (2021). *Robinhood discloses breach that exposed information of millions of customers.* CNN. Retrieved on August 4, 2022, from: https://www.cnn.com/2021/11/08/tech/robinhood-data-breach/index.html

Fiss, P. C. (2007). A set-theoretic approach to organizational configurations. *Academy of Management Review*, *32*(4), 1180–1198. doi:10.5465/amr.2007.26586092

Fiss, P. C. (2011). Building better causal theories: A fuzzy set approach to typologies in organization research. *Academy of Management Journal*, *54*(2), 393–420. doi:10.5465/amj.2011.60263120

Foreman, C. J., & Gurugubelli, D. (2015). Identifying the cyber attack surface of the advanced metering infrastructure. *The Electricity Journal*, *28*(1), 94–103. doi:10.1016/j.tej.2014.12.007

Fox, S. (2017). Beyond AI: Multi-Intelligence (MI) combining natural and artificial intelligences in hybrid beings and systems. *Technologies*, *5*(3), 1–14. doi:10.3390/technologies5030038

Fuglsang, L., & Sørensen, F. (2011). The balance between bricolage and innovation: Management dilemmas in sustainable public innovation. *Service Industries Journal*, *31*(4), 581–595. doi:10.1080/02642069.2010.504302

Fung, B. (2021). *Hackers breach Electronic Arts, stealing game source code and tools.* CNN. https://www.cnn.com/2021/06/10/tech/electronic-arts-hack/index.html

Fung, B., & Sands, G. (2021). *Ransomware attackers used compromised password to access Colonial Pipeline network*. CNN. https://www.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password/index.html

Furnari, S., Crilly, D., Misangyi, V. F., Greckhamer, T., Fiss, P. C., & Aguilera, R. (2021). Capturing causal complexity: Heuristics for configurational theorizing. *Academy of Management Review*, *46*(4), 778–799. doi:10.5465/amr.2019.0298

Furnham, A., & Boo, H. C. (2011). A literature review of the anchoring effect. *Journal of Socio-Economics*, *40*(1), 35–42. doi:10.1016/j.socec.2010.10.008

Gadzheva, M. (2007). Getting chipped: To ban or not to ban. *Information & Communications Technology Law*, *16*(3), 217–231. doi:10.1080/13600830701680537

Gonzalez, R., et al. v. Google LLC, (United States Court of Appeals for the Ninth Circuit. Docket Number. 18-16700. 2023).

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249. doi:10.1177/a017405

Grandori, A., & Furnari, S. (2008). A chemistry of organization: Combinatory analysis and design. *Organization Studies*, *29*(3), 459–485. doi:10.1177/0170840607088023

Granovetter, M. S. (1973). The strength of weak ties. *American Journal of Sociology*, *78*(6), 1360–1380. doi:10.1086/225469

He, D., Li, S., Li, C., Zhu, S., Chan, S., Min, W., & Guizani, N. (2020). Security analysis of cryptocurrency wallets in android-based applications. *IEEE Network*, *34*(6), 114–119. doi:10.1109/MNET.011.2000025

Iannacci, F., & Kraus, S. (2022). *Configurational theory: A review* (S. Papagiannidis, Ed.). Springer International Publishing. doi:10.1007/978-3-319-09450-2_23

Jarjoui, S., & Murimi, R. (2021). A framework for enterprise cybersecurity risk management. In K. Daimi & C. Peoples (Eds.), *Advances in Cybersecurity Management* (pp. 139–161). Springer International Publishing., doi:10.1007/978-3-030-71381-2_8

Jarjoui, S., Murimi, R., & Murimi, R. (2021). Hold my beer: A case study of how ransomware affected an Australian beverage company. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-6). https://doi.org/10.1109/CyberSA52016.2021.9478239

Kahneman, D., & Tversky, A. (2012). Prospect theory: An analysis of decision under risk. In *Handbook of the Fundamentals of Financial Decision Making* (pp. 99–127). World Scientific. doi:10.1142/9789814417358_0006

Katz, D., & Kahn, R. L. (1978). *The social psychology of organizations*. Wiley.

Kelleher, J. D., Mac Namee, B., & D'arcy, A. (2020). *Fundamentals of machine learning for predictive data analytics: Algorithms, worked examples, and case studies*. MIT Press.

Kelly, S., & Resnick-ault, J. (2021). *One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators.* Retrieved on August 1, 2022, from: https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

Kerner, S. M. (2022). *Colonial Pipeline hack explained: Everything you need to know*. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. doi:10.1016/j.ijcip.2019.01.001

Kuehn, A., & Mueller, M. (2014). Analyzing bug bounty programs: An institutional perspective on the economics of software vulnerabilities. SSRN *Electronic Journal,* https://doi.org/ doi:10.2139/ssrn.2418812

Landry, B. J. L., & Koger, M. S. (2023a). Exploring zero trust network architectures for building secure networks. In *Proceedings of the Decision Sciences Institute Southwest Region* (pp. 47261-47266). Academic Press.

Landry, B. J. L., & Koger, M. S. (2023b). Leveraging unified threat management based honeypots in small and midsized businesses and educational environments. In *Proceedings of the Decision Sciences Institute Southwest Region* (pp. 98301-98306). Academic Press.

Lohrke, F. T., Frownfelter-Lohrke, C., & Ketchen, D. J. Jr. (2016). The role of information technology systems in the performance of mergers and acquisitions. *Business Horizons*, *59*(1), 7–12. doi:10.1016/j.bushor.2015.09.006

Lorenz, J., Rauhut, H., Schweitzer, F., & Helbing, D. (2011). How social influence can undermine the wisdom of crowd effect. In *Proceedings of the National Academy of Sciences - PNAS* (pp. 9020-9025). National Academy of Sciences. 10.1073/pnas.1008636108

Loxton, M., Truskett, R., Scarf, B., Sindone, L., Baldry, G., & Zhao, Y. (2020). Consumer behaviour during crises: Preliminary research on how coronavirus has manifested consumer panic buying, herd mentality, changing discretionary spending and the role of the media in influencing behaviour. *Journal of Risk and Financial Management, 13*(8/166), 1-21. https://doi.org/ doi:10.3390/jrfm13080166

Mackie, J. L. (1973). *Truth, probability and paradox: Studies in philosophical logic*. Oxford University Press.

Mahoney, J., & Goertz, G. (2006). A tale of two cultures: Contrasting quantitative and qualitative research. *Political Analysis*, *14*(3), 227–249. doi:10.1093/pan/mpj017

Malecki, E. J. (2003). Digital development in rural areas: Potentials and pitfalls. *Journal of Rural Studies*, *19*(2), 201–214. doi:10.1016/S0743-0167(02)00068-2

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, *24*, 35–61. doi:10.1016/j.cosrev.2017.01.001

Matthews, L. (2021, Feb 15). *Florida water plant hackers exploited old software and poor password habits*. Retrieved on April 22, 2021, from: https://www.forbes.com/sites/leemathews/2021/02/15/florida-water-plant-hackers-exploited-old-software-and-poor-password-habits/?sh=6b0c16ca334e

Meckling, J., & Nahm, J. (2019). The politics of technology bans: Industrial policy competition and green goals for the auto industry. *Energy Policy*, *126*, 470–479. doi:10.1016/j.enpol.2018.11.031

Meyer, P. (2002). Improvisation power. *Executive Excellence,* 17-18.

MITRE Corporation. (2023). *CVE – MITRE.* https://www.cve.mitre.org

Murimi, R. (2020). Use of botnets for mining cryptocurrencies. In *Botnets* (1st ed., pp. 359–386). Routledge. doi:10.1201/9780429329913-11

National Institute of Standards and Technology. (2006). Minimum security requirements for federal information and information systems. Federal Information Processing Standards Publications (FIPS PUBS) 200. doi:10.1016/0378-7206(89)90025-6

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. In *2011 Third International Workshop on Cyberspace Safety and Security (CSS)* (pp. 21-26). IEEE. 10.1109/CSS.2011.6058566

O'Brien, S. (2021). *Robinhood's data breach involved about 7 million customers. Here's how to protect your credit from fraudsters.* CNBC. https://www.cnbc.com/2021/11/09/robinhood-data-breach-involved-7-million-clients-protect-your-credit.html

Pajunen, K. (2008). Institutions and inflows of foreign direct investment: A fuzzy-set analysis. *Journal of International Business Studies*, *39*(4), 652–669. doi:10.1057/palgrave.jibs.8400371

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611. doi:10.1016/j.cose.2011.12.010

Ponta, S., Plate, H., Sabetta, A., Bezzi, M., & Dangremont, C. (2019). A manually-curated dataset of fixes to vulnerabilities of open-source software. In *2019 IEEE/ACM 16th International Conference on Mining Software Repositories (MSR)* (pp. 383-387). IEEE Press. 10.1109/MSR.2019.00064

Ragin, C. (2008). *Redesigning social inquiry: Fuzzy sets and beyond*. University of Chicago. doi:10.7208/chicago/9780226702797.001.0001

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). Board role in cybersecurity risks. *MIT Sloan Management Review*, *59*(2), 12–15.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, D. (2020). Exploring the attack surface of blockchain: A comprehensive survey. *IEEE Communications Surveys and Tutorials*, *22*(3), 1977–2008. doi:10.1109/COMST.2020.2975999

Salemink, K., Strijker, D., & Bosworth, G. (2017). Rural development in the digital age: A systematic literature review on unequal ICT availability, adoption, and use in rural areas. *Journal of Rural Studies*, *54*, 360–371. doi:10.1016/j.jrurstud.2015.09.001

Singer, A., Anderson, W., & Farrow, R. (2013). Rethinking password policies. *Login—. The USENIX Magazine*, *38*, 14–18.

Smith, N., & Walters, P. (2018). Desire lines and defensive architecture in modern urban environments. *Urban Studies (Edinburgh, Scotland)*, *55*(13), 2980–2995. doi:10.1177/0042098017732690

Spadafora, A. (2021). *EA hack reportedly used stolen cookies and Slack to target gaming giant.* TechRadar. Retrieved on September 3, 2022, from: https://www.techradar.com/news/ea-hack-reportedly-used-stolen-cookies-and-slack-to-hack-gaming-giant

Stemwedel, J. D. (2015). *The philosophy of Star Trek: The Kobayashi Maru, no-win scenarios, and ethical leadership.* Retrieved on November 19, 2021, from: https://www.forbes.com/sites/janetstemwedel/2015/08/23/the-philosophy-of-star-trek-the-kobayashi-maru-no-win-scenarios-and-ethical-leadership/?sh=7a1285be5f48

Taylor, S. B. (2016). Can you keep a secret: Some wish to ban encryption technology for fears of data going dark. *SMU Science and Technology Law Review*, *19*(2), 216–248.

Thaler, R. H. (2018). From cashews to nudges. *The American Economic Review*, *108*(6), 1265–1287. doi:10.1257/aer.108.6.1265

Tirumala, S. S., Valluri, M. R., & Babu, G. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). 10.1109/ICCCI.2019.8821951

U. S. Department of Energy. (2021). *Colonial Pipeline cyber incident.* Energy.gov. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

Verjans, S. (2005). Bricolage as a way of life - improvisation and irony in information systems. *European Journal of Information Systems*, *14*(5), 504–506. doi:10.1057/palgrave.ejis.3000559

Winterrose, M. L., Carter, K. M., Wagner, N., & Streilein, W. W. (2016). Balancing security and performance for agility in dynamic threat environments. In *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 607-617). 10.1109/DSN.2016.61

Wu, Y., Edwards, W. K., & Das, S. (2022). SoK: Social cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 1863-1879). IEEE. 10.1109/SP46214.2022.9833757