Journal of Service Management

Cyber-attackers as a social force: conceptualizing value sabotage in cybersecurity services

Ivano Bongiovanni
The University of Queensland, Brisbane, Australia
David Goyeneche
The University of Western Australia, Perth, Australia
Elinor Tsen
The University of Queensland – St Lucia Campus, Brisbane, Australia
Edidiong Christopher James
UQ Business School, The University of Queensland – St Lucia Campus, Brisbane, Australia
Priyanka Singh
The University of Queensland, Brisbane, Australia, and
Ryan Ko
UQ Cyber Research Centre, The University of Queensland, Brisbane, Australia

Received 18 December 2024
Revised 28 July 2025
16 October 2025
27 October 2025
Accepted 8 November 2025

Abstract

Purpose – This paper examines the role of cyber-attackers as a critical social force within the cybersecurity service ecosystem. We propose a conceptual framework that integrates attackers into the traditional service triad, reframing them as attackers who influence value co-creation and service dynamics within the cybersecurity industry, particularly in the context of Cybersecurity-as-a-Service (CSaaS). We conclude that cyber-attackers represent agents of "value sabotage," a novel concept that captures how threat actors reshape service dynamics.

Design/methodology/approach – The study draws on a review of service management and cybersecurity literature, complemented by case studies of notable cyber-attacks. Building on service-dominant logic and ecosystem theory, a conceptual framework is developed, positioning attackers as influential disruptors within the CSaaS ecosystem.

Findings – The findings reveal attackers as adversarial social forces driving innovation and adaptation in the CSaaS ecosystem. An analysis of their motivations and strategies reveals how their actions compel organizations and service providers to prioritize resilience and defensive value co-creation. In turn, attackers' actions "sabotage" the value co-creation process. Our proposed framework demonstrates a transition from dyadic to triadic service interactions, incorporating attackers as critical agents.

Research limitations/implications – Future research could explore the generalizability of this framework across other industries and more specific comparisons between value sabotage and value co-destruction. Additional social forces could also be considered, such as regulators and end-customers (pentadic model).

Practical implications – The findings underscore the need for organizations to adopt adaptive service strategies that prioritize resilience, threat anticipation and collaboration to counter cyber-attacks.

Originality/value – This paper uniquely positions attackers as active contributors to the service ecosystem, extending service theory and challenging conventional notions of value co-creation in service management through the novel concept of "value sabotage." Framing attackers as malicious orchestrators of disruption, our work offers a new lens to understand how threat actors shape service design, resilience and co-creation strategies in digitally mediated service environments.

Keywords Cybersecurity, Cyber-attackers, Service ecosystem, Value sabotage, Service triad

Paper type Research article

© Ivano Bongiovanni, David Goyeneche, Elinor Tsen, Edidiong Christopher James, Priyanka Singh and Ryan Ko. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at Link to the terms of the CC BY 4.0 licence.

Journal of Service Management
Emerald Publishing Limited
e-ISSN: 1757-5826
p-ISSN: 1757-5818
DOI 10.1108/JOSM-12-2024-0537

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

1. Introduction

> If you know the enemy and know yourself, you need not fear the result of a hundred battles.
>
> Sun Tzu, The Art of War

This strategic insight resonates in today's cybersecurity landscape, where understanding cyber-attackers is essential for anticipating threats and shaping effective defense strategies (McCombie, 2018). The growing prevalence and sophistication of cyber-attacks have profoundly transformed the industry (Rundle, 2024), with ransomware attacks standing out as a pervasive and highly disruptive threat (KPMG, 2021; August *et al*., 2022). Organizations of various sizes – whether private, not-for-profit or public – are increasingly vulnerable to such attacks, yet responses from businesses and governments remain largely reactive and underdeveloped (Accenture, 2023).

For example, ransomware payments, which involve paying attackers to regain access to compromised systems, are common and generally not illegal (Sophos, 2024). At the time of writing, no country has criminalized such payments outright, except in cases where funds are linked to other illicit activities, such as terrorism (Australia Cyber Security Industry Advisory Committee, 2021a, b). In Australia, legislation such as the Cyber Security Act 2024 mandates reporting of ransomware payments and paying sanctioned entities is considered a serious criminal offense, punishable by up to 10 years in prison and substantial fines (Department of Foreign Affairs and Trade, 2021). Despite these efforts, businesses (particularly small and medium enterprises) often prioritize operational flexibility, as a ransomware attack could result in bankruptcy (Gulyas and Kiss, 2023) or, in extreme cases, loss of human lives (Hern, 2017a).

Ransomware epitomizes the power cyber-attackers wield over cybersecurity services. The rise of ransomware has prompted a range of organizational responses, including insurance companies allowing claims for ransom payments, cybersecurity executives undergoing ransom negotiation training and companies conducting tabletop simulations to improve response readiness (Mott *et al.*, 2023). These cyber-attacks are part of a broader trend of increasingly complex cyber-breaches, such as the Colonial Pipeline attack, which caused widespread fuel shortages in the USA (Reeder and Hall, 2021) and the SolarWinds breach, which infiltrated IT management software used by thousands of enterprises and government agencies globally (Alkhadra *et al.*, 2021).

Attackers employ advanced Tactics, Techniques and Procedures (TTPs) (MITRE, 2024), including AI-driven threats like deepfakes (Reina, 2024), while innovative business models such as Ransomware-as-a-Service (RaaS) allow even unskilled perpetrators to launch significant attacks by purchasing expertise from experienced cyber-criminals (Bijlenga and Kleemans, 2018; Meland *et al.*, 2020). This trend parallels servitization in other industries, where products are increasingly complemented by value-added services to drive profitability (Minaya *et al.*, 2024; Harrmann *et al.*, 2022). As a result, the cybersecurity market has expanded rapidly, with projections estimating that the global market revenue will grow at an annual rate of 7.92%, reaching 271.90 billion USD by 2029 (Statista, 2024; Shirer, 2023).

Record-breaking breaches further highlight the magnitude of cyber-attacks. For instance, the 2024 breach at Slim CD exposed the credit card details of 1.7 million individuals (Paganini, 2024), while the MediSecure hack in Australia affected nearly 12.9 million people and forced the company into administration (Jeffrey, 2024; Dickinson, 2024). The escalating arms race between attackers and defenders has made cybersecurity one of the most profitable industries of the past decade (Morris *et al.*, 2023). Globally, five cybersecurity companies appeared in 2023 in the Fortune Future 50 (Reeves and Job, 2023) and the top three (CrowdStrike, Palo Alto Networks and Fortinet) total more than 260 billion USD in market capitalization (CompaniesMarketCap, 2024).

In this market, servitization has become a strategic necessity for expanding revenue and containing costs. However, despite the growing relevance of the cybersecurity industry and its

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

constant evolution toward the "as-a-service" model, the service management literature has paid limited attention to relationships among key players in the cybersecurity ecosystem. Exceptions are rare. In one study, Malhotra and Kubowicz Malhotra (2011) define cybersecurity breaches as service failures, emphasizing the pervasiveness of the service component in the industry and ascribing the cybersecurity service model to either a triadic (buyer-supplier-end-customer) or a dyadic (supplier-end-customer) framework. Other studies have explored trust dynamics in B2B cybersecurity relationships (Pigola and de Souza Meirelles, 2024). Still, the broader service ecosystem in cybersecurity remains significantly underexamined, a gap that stands in stark contrast to the industry's rapid growth.

In the present paper, we address this gap by proposing a conceptual framework that integrates attackers into the cybersecurity service ecosystem and considers them a determinant social force (Edvardsson *et al.*, 2011). Building on recent advances in service ecosystems research (Vargo and Lusch, 2016; Lusch and Nambisan, 2015; Breidbach *et al.*, 2014), we recognize that service exchanges unfold within complex, dynamic and digitally connected ecosystems where multiple actors, resources and institutional arrangements interact. We draw on the concept of engagement platforms as physical or virtual touchpoints where actors exchange resources (Breidbach *et al.*, 2014), and we extend this perspective to examine how adversarial actors influence these interactions and reshape ecosystem dynamics. This view also aligns with Information Systems (IS) research that emphasizes how organizational and technological complexity shapes cybersecurity management and resilience (Tanriverdi *et al.*, 2025) and how real-time analytics enable agile and adaptive responses to emerging threats (Naseer *et al.*, 2024). Analyzing the interactions among suppliers, consumer organizations and attackers, we argue that these triadic relationships shape both demand and supply within the ecosystem, around the novel concept of "value sabotage." Consistent with this perspective, emerging IS work demonstrates that inter-firm and infrastructural complexity heighten cybersecurity vulnerabilities (Liang *et al.*, 2025) and highlights the behavioral and organizational implications of security practices (Pienta *et al.*, 2024), further supporting the notion that attackers exploit systemic configurations rather than isolated organizational weaknesses.

The paper is structured as follows. First, we review existing literature on service management and the role of social forces in shaping service exchange and value co-creation. We then examine the cybersecurity ecosystem and its associated business models. Next, we introduce our conceptual framework, centered around the triadic relationship and the expanded dynamics of the cybersecurity service ecosystem. We present practical examples (mini case studies) that illustrate how the triadic relationship develops in practice, reflecting the characteristics of cyber-attackers. We also propose a taxonomy for this phenomenon. Finally, we conclude the paper by highlighting theoretical and managerial implications, as well as practical recommendations and directions for future research.

This paper responds to recent calls to conceptualize service ecosystems not only as multi-actor constellations but also as digitally mediated systems where value is exchanged through technology platforms and infrastructures (Lusch and Nambisan, 2015; Breidbach *et al.*, 2014). Embedding our framework within the context of CSaaS, we extend ecosystem theory to account for adversarial actors whose primary role is to disrupt, destabilize and reshape service interactions (value sabotage), forcing providers and consumers into cycles of defensive innovation and resilience-building.

2. Literature review

2.1 Social forces in service management and cybersecurity

Traditional marketing-oriented service literature emphasizes the provider-consumer dyad, particularly in sectors where the physical and psychological environment or "servicescape," significantly affects customer experience (Rosenbaum and Massiah, 2011; Virlée *et al.*, 2020; Roy *et al.*, 2022). The servicescape is traditionally crafted to enhance customer satisfaction,

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

loyalty and engagement, thereby reinforcing a positive service experience. In this framework, value co-creation emerges through collaborative interactions, where the provider delivers value and the consumer actively shapes the experience in return (Bordian *et al.*, 2022). The dyadic model has been successfully applied in fields such as hospitality, healthcare and retail, where the direct, mutual engagement between provider and consumer defines service quality and satisfaction (Fehrer *et al.*, 2018; Wang *et al.*, 2023; Walker *et al.*, 2023). However, this dyadic focus becomes insufficient in sectors where external, hostile forces such as cyber-attackers directly disrupt service interactions, introducing complexities that challenge the conventional service framework.

As Edvardsson *et al.* (2011) contend, service exchanges and value co-creation are shaped by social forces and evolve within complex social structures. Building on this, recent work in service-dominant logic (Vargo and Lusch, 2016), service innovation (Lusch and Nambisan, 2015) and engagement platforms (Breidbach *et al.*, 2014) emphasizes that ecosystems involve multiple, interdependent actors whose interactions co-create value through institutional arrangements and resource integration. In cybersecurity, attackers function as disruptive social forces, impacting service exchanges and driving shifts in organizational strategies, industry standards and even consumer expectations. This adversarial role introduces asymmetry into the value co-creation process, as conflicting interests among the triadic actors (service suppliers, such as cybersecurity companies; service consumers, such as organizations; and attackers) reshape the dynamics of the ecosystem. Here, value creation centers on collective resilience rather than mutual benefit, demanding that both providers and consumers adopt adaptive, defensive measures not only to protect their systems but also to uphold service integrity under constant pressure from external threats (Zhang and Thing, 2021).

The inclusion of attackers as social forces within service management literature reflects the evolving complexity of digitally connected service ecosystems. Social forces are actors or institutions that influence service design, delivery and value co-creation. In cybersecurity, attackers play a significant role in shaping service dynamics. Their actions compel service providers and consumers to adapt through defensive innovation, governance reform and resilience-building. Their influence is not incidental; it is structural in the cybersecurity servicescape. Attackers disrupt the conditions under which value is created and exchanged. By recognizing them as a social force, we can account for the asymmetrical and often strategic pressures that they introduce and we can extend service theory to encompass environments where value is not only co-created but also actively contested.

The inclusion of attackers in the triadic model also fundamentally redefines service management within cybersecurity, underscoring the need for a framework that prioritizes resilience, threat anticipation and service integrity. Unlike conventional service industries, where producers and consumers collaborate toward mutual benefit, the presence of a hostile actor necessitates the ongoing evolution of protective measures. This triadic structure thus highlights the distinctive interplay between defense and value preservation, positioning cybersecurity as a complex ecosystem where value can be co-created, sabotaged and restored amid external adversarial pressures. This perspective aligns with Information Systems research emphasizing the agentic role of digital artifacts and technologies in shaping service interactions, reflecting a socio-material understanding of technological agency (Aanestad *et al.*, 2024). Shared defense mechanisms, such as threat intelligence, become central to maintaining service integrity and customer trust, with both providers and consumers actively engaged in defense against external threats. This model reflects a shift in marketing theory, where value co-creation is no longer solely about customer experience but also about mutual resilience in response to an adversarial presence (Saha *et al.*, 2021).

Among other things, the introduction of adversarial forces into the marketing environment demands a re-evaluation of core marketing principles within cybersecurity. Unlike traditional services, where value is derived from the provider's ability to enhance consumer satisfaction, cybersecurity value is tied to the provider's capacity to protect and secure the consumer's assets (Cartwright, 2014). Consequently, the effectiveness of a cybersecurity service is

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

assessed based on its success in preventing or mitigating breaches rather than on conventional customer satisfaction metrics. This shift reflects an evolution in consumer expectations, with organizations increasingly valuing cybersecurity providers for their expertise in navigating hostile environments and their ability to proactively address emerging threats (Ng and Wakenshaw, 2017; Ansari *et al.*, 2022). Accordingly, marketing strategies within cybersecurity prioritize reliability, agility and proactive security, moving away from traditional experiential aspects of service toward a focus on security-centered value creation (Konyeha, 2020; Hepfer and Powell, 2020). To lay the groundwork for our conceptual framework, the next section explores the structure and dynamics of the cybersecurity ecosystem, with a focus on the emerging CSaaS model.

2.2 Cybersecurity-as-a-service (CSaaS)

In its simplest form, the cybersecurity landscape is divided into business-to-business (B2B) and business-to-consumer (B2C) markets, although broader conceptual work emphasizes the need to see IT security and cybersecurity as part of integral, comprehensive security systems (Villalón-Fonseca, 2022). B2B cybersecurity is highly developed, driven by the need for organizations to protect vast amounts of sensitive data and adhere to regulatory standards (Trim and Lee, 2019; Abrahams *et al.*, 2024). Companies offer tailored cybersecurity solutions, ranging from firewalls and endpoint protection to AI-powered defense platforms (Heino *et al.*, 2022; Abdullahi *et al.*, 2022). In contrast, B2C cybersecurity remains less advanced, focusing primarily on basic protection for individuals, such as antivirus software and password management tools (Almansoori *et al.*, 2023; PwC, 2017). While important, B2C cybersecurity tends to be on a smaller scale, as evidenced by the Australian Signals Directorate's Annual Threat Report (2024): the average cost of cybercrimes affecting individuals is 30,700 AUD compared to businesses (49,600 to 63,600 AUD for small to large businesses). The B2C cybersecurity market lacks the sophistication, scale and institutional maturity of the B2B market.

Since the sale of the first anti-virus product in 1987, VirusScan by McAfee (Morris *et al.*, 2023), the cybersecurity ecosystem has been characterized by the constant growth of "as-a-service" offerings. Depending on variables such as risk appetite, available budgets and other contextual factors (e.g. industry, size and regulations), demand-side organizations can decide to outsource part or all of their cybersecurity requirements (Table 1, source: Morris *et al.*, 2023).

The growing trend of outsourcing cybersecurity services is evident from statistics. In a recent survey conducted by Kaspersky (2023), 41% of organizations stated they were planning to outsource their cybersecurity, with some indicating a preference for this approach over hiring additional staff (EY, 2020).

Against this backdrop, organizations specializing in cybersecurity services, such as IT providers and Managed Security Service Providers (MSSPs), are key players in the CSaaS ecosystem. MSSPs epitomize the supply of cybersecurity services: they invest in assets (e.g. technological tools) and expertise (e.g. staff) to produce top-quality cybersecurity services that they sell to clients. The clients, in turn, seek the services of MSSPs for two main reasons: to obtain production cost advantages (i.e. efficiency) and to tap into their superior expertise, technology and experience (Ding *et al.*, 2005; Reed and Scott, 2017). Through MSSPs, organizations can direct resources to revenue-generating services. In addition, given the intimate connection that exists between MSSPs and their clients (the former are fundamentally in charge of the latter's "crown jewels," the most precious data assets an organization holds), MSSPs can easily and quickly push updates and patches to the managed cybersecurity tools. This capability enables continued protection in the evolving threat environment and, ultimately, supports the organization's business continuity and compliance with relevant legislation (Slapničar *et al.*, 2023). On their end, MSSPs tend to serve broad client bases, which translates into increased exposure to novel, emerging cyber-threats. This exposure enables

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

Table 1. Examples of different CSaaS types

Service	Description	Examples of services
Security personnel	Contracting out services associated with specific roles, either strategic or more operational/technical	Chief Information Security Officer (CISO) (including so-called virtual CISO), forensics specialist, pentester
Cybersecurity training	Training programs and courses intended to raise cyber-awareness within organizations and/or limit the impact of data breaches	Webinars, workshops, phishing campaigns, regulatory compliance training, desktop exercises
Vulnerability assessment	Systematic identification, measurement, and categorization of weaknesses within an organization's systems	"Patching" requirements, corporate security policies, remote access
Periodic penetration testing	Simulated attacks, performed by highly skilled personnel, with a view to 'stress-test' an organization's IT systems and find vulnerabilities before exploitation	Penetration testing
E-mail security	Services aimed at protecting corporate email accounts, one of the biggest gateways to organizations	Spam filters, digital signatures, email encryption
Identity and Access Management	Mapping and protection of corporate identities and accounts, to prevent take-over and malicious usage	User registration, assignment of roles and privileges, Multi-Factor Authentication (MFA)
Cyber-insurance	One of the most outsourced security functions, it entails sharing the financial impact of cybersecurity risks with a third-party provider	–
Incident response	The ability to rely (often 24/7) on third-party providers who intervene 'boots-on-the-ground' to assist in case of a data breach	Security Operations Centre, cyber-crisis team
Business continuity and disaster recovery planning	Longer-term interventions aimed at bringing the organization to the pre-event stage	Recovery plans
Security information and event management (SIEM)	Detection and investigation of events to identify genuine threats and distinguish them from false positives	Security Operations Centre, SIEM platforms
Patching and updates	Upon disclosure of system vulnerabilities, remediation is performed through application of patches and updates	Software and configuration updates, operating systems patching
Compliance with security standards	Often outsourced to consultants with expertise in the governance, risk and compliance space (GRC), these services aim at aligning the organization with cybersecurity best practices	ISO/IEC 27001, NIST Cybersecurity Framework

Source(s): Authors' own work

them to continuously improve the quality of their services (Wang *et al.*, 2018). While this outlines the operational landscape of CSaaS, it is essential to situate these interactions within the broader service ecosystem literature to understand how adversarial forces reshape service dynamics.

Recent scholarship has emphasized that service interactions no longer unfold solely within dyadic or triadic exchanges but within complex, digitally connected ecosystems where actors co-create value through dynamic configurations of resources, institutional arrangements and engagement platforms (Vargo and Lusch, 2016; Lusch and Nambisan, 2015; Breidbach *et al.*,

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

2014). Service ecosystems extend beyond bilateral relationships to include the technological, social and institutional structures that shape and constrain interactions, with digital platforms acting as critical enablers of resource integration, coordination and value exchange (Breidbach and Brodie, 2017). While this body of work has largely focused on constructive interactions and positive value co-creation, limited scholarly attention has been given to adversarial or malicious actors who disrupt these systems and drive value co-destruction. Extending this literature, we position cyber-attackers as adversarial actors whose sabotage of value co-creation reconfigures service interactions and drives institutional and strategic adaptation within CSaaS ecosystems.

In the present research, we argue that any framework aiming to capture the dynamics of the CSaaS ecosystem is significantly incomplete without accounting for the role of cyber-attackers as social forces shaping service exchange and value co-creation through value sabotage (Pienta *et al.*, 2024). In this space, literature is at best scarce. In the field of cybersecurity economics, game theory is one of the frameworks that model attacker-defender behaviors with a view to predicting adequate investments for the latter (Feng *et al.*, 2019; Wu *et al.*, 2015). Feng *et al.* (2019) have adopted a system dynamics approach to develop a model that explains the complex relationships driving cybersecurity investments by MSSPs. A core component of their model revolves around factors associated with attacks. Among these, motivation for attacks, perceived vulnerability of target organizations and availability of attack tools stem directly from attackers' motivation, resources and expertise. We now present the conceptual framework of our study through a detailed examination of the attackers' role in shaping the CSaaS ecosystem.

3. Proposed conceptual framework: CSaaS as a triadic relationship

Our review of the service management and cybersecurity literatures reveals that CSaaS can be modeled as a complex network of interactions among:

(1) Suppliers of cybersecurity services (e.g. MSSPs), who meet the entirety or part of the cybersecurity requirements of client organizations (see Table 1);

(2) Organizational consumers of cybersecurity services, who outsource cybersecurity services (e.g. to MSSPs) for efficiency and effectiveness (e.g. legal compliance) purposes;

(3) Cyber-attackers, who function as a social force impacting the service exchange and value co-creation dynamics between suppliers and consumers. In this paper, we introduce the novel concept of *value sabotage* to describe the nature of this impact.

The resulting conceptual framework is illustrated in Figure 1.

Our framework posits that attackers are, in fact, indirectly orchestrating the CSaaS value co-creation and service exchange processes through their attacks. This proposition contrasts with prior work on service orchestrations (Breidbach *et al.*, 2016), which positions attackers as malicious orchestrators undermining the goals of the actors involved in CSaaS. Through value sabotage, attackers influence the value co-creation and service exchanges between cybersecurity suppliers and organizational consumers. The resulting dynamic is one of a constant "arms race" in both international relations (Craig and Valeriano, 2016) and organizational contexts (Palma, 2024).

Different attackers will likely have varying impacts on value co-creation and service exchange in CSaaS, resulting in distinct value sabotage configurations. These responses reflect the fact that an actor's reaction to a cyber-attack depends on the attacker's strategic intent, shaped by their motivation, skill level and resources (Feng *et al.*, 2019). Hence, attackers not only disrupt the relationship between the supplier and the organization but also force both sides to continually adapt to new threats. This may be through new services, altered relational dynamics or shifts in demand. So, how do different types of cyber-attackers impact

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

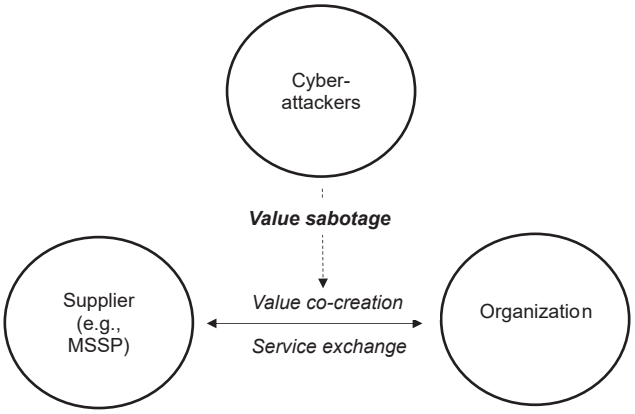

Figure 1. Our conceptual model, the CSaaS triad and the novel concept of value sabotage. Source: Authors' own work

the creation and consumption of cybersecurity services in our triadic model? We illustrate this question in the next section.

4. Cyber-attackers: typologies and impact on CSaaS

AT&T's MSSP (Level Blue) classifies four extrinsic and three intrinsic motives for cyber-attacks: among the former, financial, espionage, war/defense and facilitation to other targets; among the latter, social/political "hacktivism," revenge and destruction (Mark, 2024). Statistics show that, overwhelmingly, cyber-attackers are motivated by financial gain, seeking to profit through methods such as ransomware, data theft and fraud (Bongiovanni *et al.*, 2022; Ablon, 2018). Some attackers are also driven by political or ideological reasons, aiming to disrupt or draw attention to specific causes through hacktivism (Snider *et al.*, 2021; Cayubit *et al.*, 2017).

The skills and expertise required to perpetrate a cyber-attack have also dramatically changed in recent decades: at the dawn of the Internet era, *hacking* required complex technical skills, which significantly limited its scale. Nowadays, the business models associated with cyber-criminal activity have evolved. Organized crime groups have become prominent players in a thriving Attack-as-a-Service (AaaS) ecosystem (Huang *et al.*, 2017). Sourced from the *dark web* (Bongiovanni *et al.*, 2022), AaaS platforms provide comprehensive resources, including ransomware kits, phishing tools and botnets, to execute sophisticated attacks. Operating in this framework allows even those without deep technical expertise to perpetrate cybercrimes, creating a robust marketplace that reduces barriers to entry for potential attackers (Huang *et al.*, 2017; Brooks *et al.*, 2021). The demand for AaaS, in turn, incentivized organized crime groups to professionalize their operations, creating modular, scalable cyber-attack services that cater to various malicious intentions, from financial gain to political sabotage.

As anticipated in our triadic framework, these dynamics have substantial implications for suppliers of cybersecurity services (e.g. MSSPs), who face mounting challenges as cybercriminals target both their clients and the providers themselves. Cyber-attacks that exploit financial institutions, for instance, can lead to market fluctuations, influence investor confidence and damage corporate reputations. For MSSPs, the direct impact is the increased pressure to evolve their threat intelligence, defensive capabilities and crisis response frameworks to keep pace with evolving cybercrime strategies (Li and Liu, 2021). Additionally, as organized crime groups expand their operations, MSSPs must contend with the potential of insider threats and breaches targeting the very systems meant to secure clients. This highlights their critical role in safeguarding against a continuously adaptive cybercrime landscape.

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

There are five generally accepted categories of cyber-attackers (Table 2): state-nexus actors, cybercrime actors, private sector offensive actors, hacktivists and script kiddies (ENISA, 2024). Given their relevance to the service ecosystem, we also add malicious insiders to this list (Homoliak *et al.*, 2019). For completeness and due to their ability to influence the cybersecurity service ecosystem, we also mention negligent insiders as an additional category. These cannot, however, be defined as cyber-attackers due to a lack of intentionality in their actions (Dupuis and Khadeer, 2016) and will therefore be excluded from our analysis.

These six categories represent the social forces impacting the CSaaS ecosystem and influencing value co-creation and service exchange between suppliers and organizations, through value sabotage. Their activities illustrate the varying levels of sophistication and methodologies employed in cyberattacks, providing a detailed understanding of the threat spectrum. Moreover, categorizing these groups highlights their distinct roles in CSaaS and allows us to address a broader scope of cybersecurity challenges, offering clearer insights into their impact on the service industry.

The first category, *state-nexus actors*, includes any state or military-sponsored or affiliated actors. Generally, these actors are motivated by geopolitical conflicts (Hald and Pedersen, 2012) to maintain or promote state ideologies and threaten other states' ideologies. This motivation may lead them to target government agencies and critical infrastructure (Sailio *et al.*, 2020). These actors typically have medium-to-high levels of skill and experience, with access to substantial resources (de Bruijne *et al.*, 2017; ENISA, 2024). Their business models vary and some form structured networks or outsource operations to private sector offensive actors or *hacker-for-hire* groups (ENISA, 2024; Sailio *et al.*, 2020). Importantly, due to the potentially extensive resources at their disposal and their strong motivation, state-nexus actors can introduce systemic shocks into the supplier-organizational consumer relationship (Craig and Valeriano, 2016). In these cases, commercial logic alone may be insufficient for reconfiguring and innovating cybersecurity services.

Private sector offensive actors are organized groups equivalent to legitimate entities (ENISA, 2024). Chng *et al.* (2022, p. 6) note that these actors "perform sophisticated attacks using the full repertoire of attack vectors and customized code/scripts," implying that these actors typically have expert skills. In addition, these actors are increasingly organizing themselves in pseudo-entities, giving them greater scope while providing many of the benefits that legal entities experience when they commercialize. One notable example is NSO Group, an Israeli cyber-intelligence firm known for providing governments with spyware for espionage (Kirchgaessner, 2024a). In another case, an Austrian data firm was accused of selling malware and conducting cyber-attacks on behalf of clients (Scroxton, 2022). They are similar to state-nexus actors, but potentially to a lesser extent, given their level of specialization. These actors can challenge the integrity of service exchange and the associated governance structures.

Hacktivists are ideologically motivated individuals (de Bruijne *et al.*, 2017), willing to create awareness and notoriety around a chosen issue. The experience and skill level of hacktivists may vary, but they are considered to have lower skill levels than cybercrime actors or private sector offensive actors (de Bruijne *et al.*, 2017; Hald and Pedersen, 2012). Hacktivists can act as institutional entrepreneurs (Tiberius *et al.*, 2020) who are motivated to reconfigure existing institutions and realign their value propositions in favor of personal causes.

Script kiddies are generally novice hackers or attackers who leverage existing tools and scripts to attack organizations, mainly for demonstrative purposes (e.g. "bragging rights" amongst peers) (Hald and Pedersen, 2012). With generally low levels of skill (Chng *et al.*, 2022), their actions can nonetheless expose vulnerabilities and cause reputational harm. Such breaches can diminish trust in cybersecurity providers and prompt clients to reassess service effectiveness.

Cybercrime actors or hack-for-hire actors are any other attackers motivated by financial gain (ENISA, 2024). The most prominent group, cybercrime actors, is motivated by their own

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

Table 2. Cyber-attacker types and their influence on CSaaS

#	Attacker type	Main target (consumers or organizations)	Description	Attack motivations	Business model/ skill level	Typical tactics, techniques, and procedures	Impact on supplier-consumer relationships (value sabotage)	Impact on CSaaS	Examples of impact on CSaaS
1	State-nexus actors	Other states and organizations (ENISA, 2024)	State or military-sponsored actors typically with significant time, funding, and resources available to gather intelligence and cause interference (ENISA, 2024)	Undermine geopolitical rivals, gather intelligence, disrupt critical infrastructure, exert political or military pressure	Advanced and expert skills (de Bruijne *et al.*, 2017); associated with existing state or military operations	Spear-phishing password attacks, social engineering, direct compromise, data exfiltration, remote access trojans, and destructive malware (Center for Internet Security, 2024)	Introduce systemic shocks: commercial logic insufficient to guide cybersecurity service configurations	The potential damage from state-nexus actors can make cyber-insurance services *unapplicable* (Mascellino, 2022).	Cyber-insurance coverage reduced for *acts of war* (Cremer *et al.*, 2024)

(*continued*)

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on 27 May 2026

Table 2. Continued

#	Attacker type	Main target (consumers or organizations)	Description	Attack motivations	Business model/ skill level	Typical tactics, techniques, and procedures	Impact on supplier-consumer relationships (value sabotage)	Impact on CSaaS	Examples of impact on CSaaS
2	Private Sector Offensive actors	Organizations	"Commercial entities that engage in the cyber-surveillance industry" (ENISA, 2024, p. 20)	Conduct espionage, collect sensitive corporate data, offer surveillance or sabotage services for paying clients	Advanced and expert skills; act like a typical professional services business (ENISA, 2024)	Phishing, social engineering, business email compromise (BEC) scams, botnets, password attacks, exploit kits, malware, ransomware (Center for Internet Security, 2024)	Focus on intelligence-related information, expansion of associated cybersecurity services	Collaboration amongst defenders is critical to combat the significant expertise and skills of these actors (Ackerman, 2021)	MITRE ATT&CK Framework: a collaborative, open-source taxonomy of adversary tactics and techniques (MITRE, n.d.)
3	Hacktivists	Organizations (often governments or critical infrastructures)	Motivated by the desire for political or social change to disrupt organizations to make an ideologically driven statement (ENISA, 2024; Hald and Pedersen, 2012)	Raise awareness, protest perceived injustices, embarrass or expose organizations, promote ideological agendas	Varying levels of skills and business model sophistication (ENISA, 2024); tends to function on a smaller scale	DDoS, doxing, website defacements (Center for Internet Security, 2024)	Act as institutional entrepreneurs (Tiberius *et al.*, 2020) to reshape norms and expectations within service ecosystems	Unregulated "white hat" hacking has led organizations to set clear boundaries and rules around disclosure (HackerOne, 2021)	Bug bounty programs (Zhang *et al.*, 2024)

(*continued*)

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on 27 May 2026

Table 2. Continued

#	Attacker type	Main target (consumers or organizations)	Description	Attack motivations	Business model/ skill level	Typical tactics, techniques, and procedures	Impact on supplier-consumer relationships (value sabotage)	Impact on CSaaS	Examples of impact on CSaaS
4	Script kiddies	Consumers/ organizations	An attacker with limited experience relying on pre-made scripts for hacking; may have various motivations (Hald and Pedersen, 2012)	Experiment, gain peer recognition, demonstrate skills, cause disruption for personal satisfaction or entertainment	Typically, have little experience and knowledge on attack tools; not a clear business model	SQL injections and various scripts (Center for Internet Security, 2024)	Expose eminent vulnerabilities to contribute to shaping the cybersecurity service ecosystem	Script kiddies' activities have raised awareness on the ease-of-use of off-the-shelf attack tools and techniques (Temple-Raston, 2022). Gen AI has powered this further	Individual cybersecurity solutions to counter the increased availability of hacking scripts
5	Cybercrime actors/ Hacker-for-hire actors	Consumers/ organizations	Motivated by financial gain to develop opportunistic attacks (i.e. extortion or monetization of information gathered) (ENISA, 2024)	Steal money or assets, demand ransoms, sell stolen data, conduct attacks for hire	Varying skills (ENISA, 2024); typically exist as syndicates, contractors or small groups	Phishing, social engineering, deepfakes, business email compromise (BEC) scams, botnets, password attacks, exploit kits, malware, ransomware (Center for Internet Security, 2024)	Influence competition in cybersecurity suppliers' markets; contribute to driving innovation	The threat of a sophisticated attack led to a greater demand for cyber-threat intelligence (Bromiley, 2016)	Expansion of cyber-threat intelligence offerings by suppliers (Sun *et al.*, 2023)

(*continued*)

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on 27 May 2026

Table 2. Continued

#	Attacker type	Main target (consumers or organizations)	Description	Attack motivations	Business model/ skill level	Typical tactics, techniques, and procedures	Impact on supplier-consumer relationships (value sabotage)	Impact on CSaaS	Examples of impact on CSaaS
6	Malicious insiders	Organizations	Cyber-attacks perpetrated by "... authorized users who have legitimate access to sensitive/ confidential material, and they may know the vulnerabilities of the deployed systems and business processes" (Homoliak *et al.*, 2019, p. 30)	Various motivations, but mainly financial, political, personal (e.g. revenge by disgruntled employees)	Level of skills can vary depending on position and degree of access to privileged information; typically, lack of specific business model	Malicious code (e.g. malware) or intentional disclosure (Homoliak *et al.*, 2019)	Breach trust within service systems; undermine internal value co-creation and necessitate stronger identity and access management	Expansion of cybersecurity services protect organizations from insiders' threats	Expansion of identity and access management solutions (IAM)

Source(s): Authors' own work

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on 27 May 2026

personal financial gain generated through theft, extortion or other monetization strategies (ENISA, 2024). As cybercrime and hack-for-hire actors are primarily motivated by financial gain, they exploit any vulnerability (Sailio *et al.*, 2020), leading to a scattergun approach. Cybercrime actors may work alone but are increasingly observed as working in groups or networks (e.g. a cyber syndicate) (ENISA, 2024). Similarly, hacker-for-hire actors may also work with other actors, but, unlike cybercrime actors, they are usually hired by other criminals to provide hacking services. Their motivation, resources and capabilities make their role eminent in influencing competitive dynamics within the cybersecurity service ecosystem. To counter cybercrime actors and stay ahead of the competition, suppliers must constantly innovate (Naseer *et al.*, 2024).

Malicious insiders are authorized users who exploit their access to organizational IT assets to perpetrate attacks of various types (Homoliak *et al.*, 2019). Their motivations can vary, but usually encompass financial gain, political reasons (e.g. to challenge the status quo within their employer organization) or personal motives (e.g. disgruntled employees or former employees willing to execute an act of revenge against their employer or former employer). Skills and capabilities also depend on circumstances. Malicious insiders often exploit sub-optimal identity and access management systems, leaving organizations unable to fully control access to organizational assets (e.g. networks, data). Unlike negligent insiders, who act without intention (e.g. through negligence, lack of skills or inaction), malicious insiders engage in deliberate actions to cause harm to a target organization.

4.1 How do cyber-attackers impact CSaaS: emerging dynamics and six illustrative scenarios

In this section, we first offer insights into how cyber-attackers influence suppliers, organizational consumers and the value co-creation/service exchange between them, through value sabotage. In doing so, we examine the dualistic dynamics that emerge amongst the three components of the triad. We then use publicly available data to illustrate how attackers' activities (e.g. attack strategies, business models, involved parties) constitute social forces that shape the CSaaS ecosystem.

Cybersecurity service provision has moved from a traditional reactive approach to counter cyber-criminals' activity to a more proactive one. The recent evolution of Cyber Threat Intelligence as a service epitomizes this trend (Smith and Ingram, 2017; Sun *et al.*, 2023). From its origins as a reactive and isolated activity in response to cyber-incidents caused by "worms," viruses and basic malware (1990s, with Computer Emergency Response Teams (CERTs) as protagonists), through steps toward more structured threat intelligence by means of proactive detection and prevention (early 2000s, with the emergence of Security Information and Event Management systems), CTI has now become a proactive endeavor. Since the 2020s, machine learning has been integrated to foster automated threat intelligence, providing real-time, curated and contextualized data to cybersecurity teams within organizations. The evolution of CTI cannot be separated from the evolving behaviors of cyber-attackers. Script kiddies and hackers seeking visibility have been partially replaced by well-organized, money-driven cyber-criminals who leverage technology like (and probably better than) cyber-defenders. Suppliers have had to adapt. Well-organized and connected networks of corporate vendors have multiplied the cybersecurity services traditionally offered by more or less formal communities of CERTs and similar not-for-profit organizations (Zrahia, 2018).

Organizational consumers have adapted too, in response to the shifting dynamics of the ecosystem and the attackers. Several factors have contributed to increased exposure to cyber-attacks, such as the expansion of organizations' digital footprints and the growing availability of cyber-attack tools (Malatji and Tolah, 2025). This has led organizations to increase their cybersecurity expenditure. Estimates indicate that the global cost of cybercrime has grown from 0.86 trillion USD in 2018 to 10.29 trillion USD in 2025 (Statista, 2025). Sub-functions in

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

cybersecurity departments have also multiplied, with increased specialization and a mix of in- and out-sourcing arrangements. Common cybersecurity functions include security engineering, identity management, security operations, threat intelligence, security architecture, etc (Allen *et al.*, 2015). Another example that epitomizes the evolution from the organizational consumers' perspective is the activities of blue, red and purple cybersecurity teams (Malatji and Tolah, 2025). Blue teams traditionally focus on defending an organization. In recent years, their role has been complemented by red teams, whose main goal is to attack an organization, with a view to unveiling its vulnerabilities and fixing them. The specialization of these two teams has led to a compartmentalized approach, requiring the creation of a bridge: purple teams. This team's main task is to facilitate collaboration between defensive and offensive efforts to improve cyber-resilience.

Finally, the service exchange between suppliers and organizational consumers is impacted by cyber-attackers' actions. This creates dual dynamics within the triad that we will briefly explore here. In our opinion, the core element of such dynamics resides in the perceived advantage or "edge" that cyber-attackers seem to generally have over defenders. For example, Atrews (2020) discusses how zero-day exploits allow attackers to strike before vulnerabilities are even known, making defense extremely difficult. Another study by Cremer *et al.* (2022) highlights how AI enables attackers to automate and scale their operations faster than defenders can respond.

Collaboration between suppliers and organizational consumers, therefore, becomes a necessity to address the gap and increase the defenders' chances to "win." Once more, cyber threat intelligence offers an example of this. To protect organizational consumers, suppliers share anonymous, strategic and technical data (e.g. Tactics, Techniques and Procedures of threat actors to study their behaviors and actions; Indicators of Compromise to identify breaches; etc.) they collect from other organizations. To enrich such data and maintain its quality and relevance, organizational consumers contribute their own information. As such, the cyber threat intelligence ecosystem exhibits a small-world structure, where information-sharing relationships are characterized by coopetition (Zrahia, 2018).

One of the main drivers of investments in service improvements by cybersecurity suppliers is the evolving attack techniques of cyber-attackers. For example, incident response organizations are continuously expanding their offerings as attacks become increasingly sophisticated (Al Maamari *et al.*, 2024). These firms now provide faster threat detection, deeper forensic analysis and more robust recovery protocols. Their service evolution is driven by lessons learned from real-world breaches, helping them better anticipate and neutralize future threats.

Lastly, the relationship between attackers and organizational consumers is impacted by the effectiveness of the former in compromising the defenses of the latter, either directly or through the performance of the suppliers. With degraded performance, consumers are more likely to "switch" to other suppliers or to insource cybersecurity functions, thereby contributing to shaping competitive dynamics.

Fragmentation in cybersecurity markets is currently high (Mordor Intelligence, 2025). Cai and Zhang (2025), for example, argue that cybersecurity is a quasi-public good, and the imbalance between supply and demand results in high fragmentation. Aggregation is also a recent, limited trend, driven mainly by platformization and mergers and acquisitions. Symantec's acquisition of data storage company Veritas in 2005 was one of the first significant acquisitions in history (Stiennon, 2020). As a consequence of the multiplication of the TTPs adopted by cyber-attackers, the increased complexity of cybersecurity products and services has resulted in enhanced specialization by suppliers, partially countering the simultaneous aggregation trends observed in the industry. The net result is a current market dominated by fragmentation, with pockets of larger players acting as aggregators (e.g. Google, AWS) (Strategy of Security, 2022).

At first glance, the relationship among suppliers, organizational consumers and cyber-attackers might appear to be one of value co-destruction – the process by which interactions

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

between service systems lead to a reduction in one or more parties' well-being. This concept, as defined in service-dominant logic (Plé and Chumpitaz Caceres, 2010), typically refers to unintended or emergent outcomes arising from misaligned goals, poor coordination or systemic vulnerabilities. However, this framing becomes problematic when applied to cybersecurity. Cyber-attackers do not merely participate in a dysfunctional service interaction; rather, they deliberately operate to exploit, disrupt and degrade the value co-created between legitimate service systems. Their actions are not accidental byproducts of systemic misalignment but are purposefully orchestrated to inflict harm.

This intentionality introduces a critical distinction. Traditional definitions of value co-destruction, such as "an interactional process between service systems that results in a decline in at least one of the systems' well-being" (Lumivalo *et al.*, 2024), fail to account for the asymmetry and malevolence inherent in cyber-attacks. In cybersecurity, the attacker is not a co-creator of value gone rogue, but an agent whose objectives are antagonistic to the service ecosystem. As such, the framework of value co-destruction may be insufficient to fully capture the dynamics at play. Instead, we argue that there is a need to conceptualize a parallel construct, "value sabotage," that explicitly incorporates the role of adversarial behavior in the service literature. We now examine six illustrative scenarios to better examine how value sabotage operates, categorizing them by cyber-attacker types. In these scenarios, we investigate the specific mechanisms of value sabotage at play.

State-nexus actors: The Mondelez vs Zurich case linked to the NotPetya ransomware attack is an example of how a state-nexus cyber-attack led to a significant shift in cybersecurity service offerings. This case relates to cyber-insurance services and the so-called *act of war* exclusion clause. In this case, Zurich is the CSaaS supplier and Mondelez the client organization.

In 2017, a ransomware attack (NotPetya) targeted critical Ukrainian infrastructure, such as banks and airports (Poireault, 2023). The attack propagated across networks, reaching global organizations (BBC, 2018). As a result of NotPetya, many systems and devices were shut down, causing significant data and monetary losses (US Cybersecurity and Infrastructure Security Agency, 2018). Among the affected companies, Mondelez International (Greenberg, 2018; Wan, 2020) suffered operational damage, including over 1,500 servers and 20,000 laptops made unusable (Adriano, 2022). Notably, attackers were not motivated by money. Hern (2017b, p. 1) notes that "the ransomware was coded in such a way that, even if users did pay up, their data could never be recovered." This approach to ransomware indicated that the attackers were likely motivated by other reasons beyond financial (Alvarez, 2017). NotPetya was later attributed to the Russian military (US Cybersecurity and Infrastructure Security Agency, 2018).

This attribution led to issues associated with cyber-insurance. Because the damage incurred from NotPetya exceeded 100 million USD (Mascellino, 2022), Mondelez International submitted a claim to its insurer, Zurich. At the time, Mondelez International had an "all-risk" property insurance policy, which nonetheless contained an *act of war* exclusion (Wan, 2020): given their unpredictability, the power imbalance between the involved parties and the potential losses, cyber-attacks considered *acts of war* are usually not covered by cyber-insurance. Prior to this attack, cyber-attacks had typically not been treated as *acts of war*. However, in this instance, Zurich claimed that NotPetya was effectively an *act of war* (attribution to the Russian military, Adriano, 2022). Mondelez's counterargument claimed that this was not an act of war: the Ukrainian infrastructure was the real target, with Mondelez International seen as "collateral damage" (Smalley, 2022, p. 1). The ensuing lawsuit was settled five years later, with minimal information provided on the settlement terms (Mascellino, 2022).

As a result of this attack, cyber-insurers started shifting their services to exclude specific cyber-attacks, such as those committed by state-nexus actors (Mascellino, 2022). For example, Lloyd's has since adjusted its war exclusion policy to cover only losses that arise from computer systems in countries deemed the "impacted state" (Di Marco, 2023). This case

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

epitomizes how state-nexus actors operate value sabotage, introducing systemic shocks into the cybersecurity service ecosystem that make commercial logics insufficient. Cyber acts of war are thus increasingly seen as non-addressable through commercial services such as cyber-insurance.

Mechanisms of value sabotage: In this scenario, value sabotage was motivated by geopolitical reasons. The impact it had was systemic and indirect, in that the threat actors did not intend to target the service provider (Zurich). Value sabotage unfolded as collateral damage from the disruption of governance structures that threat actors had caused (i.e. the attribution of the attack to a state actor forcing insurers to reconsider liability and risk models, undermining the predictability of service contracts and, consequently, trust in insurance mechanisms). On this same note, the operational damage that Mondelez suffered was, similarly, indirect (1,500 servers and 20,000 laptops).

Private sector offensive actors: NSO Group is alleged to be an Israeli cyber-weapons development group supporting national security (Westendorf, 2021). Despite their claims of supporting national security, NSO Group has developed spyware that can breach the mobile defenses of many devices through their Pegasus app. The Pegasus app has also allegedly been sold to various governments, raising concerns about its misuse for surveillance purposes (Ackerman, 2021). In 2019, litigation arose between NSO Group and WhatsApp (Kirchgaessnar, 2024b). This lawsuit centered on the actions of NSO, which leveraged a vulnerability in WhatsApp to install spyware on the phones of over 1,400 users (e.g. journalists, human rights defenders, religious figures, previous victims of cyber-violence, etc.) (Hopkins and Kirchgaessner, 2019). The lawsuit is currently ongoing, with NSO Group recently required to hand over their code (Kirchgaessnar, 2024b). Despite the lack of a current settlement, former US President Biden imposed a ban on NSO products in 2021 (Panagiotopoulos, 2024). The ban remains in effect despite lobbying efforts and the release of a transparency report by NSO Group (Panagiotopoulos, 2024).

In response to the value sabotage activities of private sector offensive actors, the cybersecurity industry has seen more openness, transparency and collaboration. Such a shift is major in cybersecurity, where confidentiality and secrecy are often a necessity. As noted by Ackerman (2021), collaboration between the cybersecurity services industry and other stakeholders has become more critical, indirectly due to the rise of such actors.

Mechanisms of value sabotage: Unlike the previous scenario, in this case, value sabotage was direct, in that NSO Group deliberately targeted WhatsApp, compromising a widely used digital platform. Their operation was covert, as their ultimate goal was to install spyware through WhatsApp vulnerabilities. Commercial and political dynamics were involved in this case, given NSO Group's alleged support for national security.

Hacktivists: Hacktivism is typically motivated by non-monetary reasons, to gain media attention and attract focus on specific issues (e.g. organizational, ethical, religious, political, etc.). A famous case of hacktivism is the Intel "hacking" by Randal Schwartz (1997). In 1993, Schwartz was an Intel employee and was voluntarily investigating the security of his company. He installed a program to guess employees' passwords on Intel's machines and managed to "crack" 50 passwords, indicating poor password practices among Intel employees. Schwartz did not report the issue but instead kept trying to guess more passwords. Schwartz later stated that his motivation was to "show Intel they were incompetent" (Schwartz, 1997, p. 1). A legal procedure ensued against Schwartz, who was found guilty of illegally breaking into a computer system.

In discussions about Schwartz's actions and Intel's response, many programmers were sympathetic to Schwartz (1997). Hence, finding computer vulnerabilities was considered acceptable in hacking groups. The resulting legal action led some individuals to be less willing to disclose any vulnerabilities they discovered in organizations' cybersecurity defenses (Lewis, 1995). Despite the Schwartz case, numerous organizations started seeing the importance of having their networks and systems constantly "stress-tested." This led to the creation of the so-called bug bounty programs, where security researchers and *hackers*

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

external to an organization (called *ethical hackers* or *white hats*) identify and report security vulnerabilities without fear of legal action (Arshad *et al.*, 2024). Essentially, these programs encourage white hat hacking using remuneration, helping to improve the cybersecurity of organizations, while acting within specific boundaries set by the organization itself (e.g. vulnerabilities generally cannot be disclosed to the public) (HackerOne, 2021).

Bug bounty programs are an example of a cybersecurity service created because of the action of hacktivists and their willingness to identify vulnerabilities in organizational networks.

Mechanisms of value sabotage: Typical of hacktivists' actions, Schwartz operated in the "gray" zone at the intersection of actions that are intentional and have an underlying positive goal (exposing inadequate password protection practices) and those that are ethically ambiguous (challenging of Intel's internal governance structures). His actions resulted in an erosion of trust in corporate norms and policies and, overall, reputation. The case also resulted in attempts to "legally protect" previously unregulated areas (ethical hacking practices). Sabotage, in this sense, took a more nuanced form than traditional adversarial operations (see the other scenarios).

Script kiddies: A notable case illustrating the role that script kiddies play as a social force in the CSaaS ecosystem is the 2015 TalkTalk data breach. TalkTalk is an Internet Service Provider based in the United Kingdom (TrendMicro, 2015). In 2015, attackers used a disclosed vulnerability to access TalkTalk"s data (Press Association, 2016). Little effort was required from the attackers as the original individual who had discovered the vulnerability had widely shared its details. The limited effort required is a notable characteristic of script kiddies.

In 2015, a 17-year-old discovered a vulnerability on TalkTalk's website and shared their discovery online (Press Association, 2016). This led to other individuals exploiting this vulnerability, gaining access to the personal data (for some, even bank account details) of 156,959 customers (ICO, 2016). The exploit used was a simple SQL injection, which does not require significant effort or expertise to implement. According to the United Kingdom's Information Commissioner's Office (Hern, 2016), "SQL injection is well understood, defenses exist, and TalkTalk ought to have known it posed a risk to its data". Given the simplicity of the attack needed to access a large amount of data, it was demonstrated that TalkTalk lacked appropriate cybersecurity maturity. This lack of maturity was reflected in the 400,000 GBP fine that the company received, which at the time was the highest fine imposed by the United Kingdom's Information Commissioner's Office (Hern, 2016). This and similar attacks have demonstrated that data breaches can have long-term impacts not only on the affected organization but also on its end-customers.

Mechanisms of value sabotage: The most prominent aspect of this case of value sabotage was the visibility that the script kiddies' actions received. The perpetrator publicly announced the vulnerability they had identified to raise awareness. Once more, the action resulted in trust erosion for TalkTalk. This degraded the value co-created between TalkTalk and its customers, leading to potential customer churn. The motivation behind this action can be defined as opportunistic, as the perpetrator used a relatively simple exploit.

Cybercrime actors/Hackers-for-Hire: Examples of this type of attacker abound in the literature, but one prominent case was the 2016 Bangladesh Bank heist incident. Mercenary group Lazarus was hired by the North Korean government to steal funds from the Bangladesh central bank through the SWIFT financial system. The Lazarus Group's cyber-criminals breached the bank's computer systems and exploited vulnerabilities in the SWIFT international money transfer network (O'Grady and Malone, 2022). The Group managed to initiate fraudulent transfers, attempting to steal nearly 1 billion USD from Bangladesh's account at the Federal Reserve Bank of New York. They successfully siphoned off 81 million USD, redirecting the money to various accounts in the Philippines (BBC, 2021). The scheme was only partially uncovered when a transaction detail error (a misspelled name) raised red flags and halted further transfers. The heist exposed serious weaknesses in the global financial infrastructure, particularly within the SWIFT system that connects financial institutions

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

worldwide (Kabir, 2023). Although much of the stolen money was funneled through casinos and laundered through complex schemes, significant portions remain unaccounted for, further validating our argument on the crucial importance of attackers in shaping value co-creation and service exchange in the CSaaS ecosystem, through value sabotage.

Mechanisms of value sabotage: Typical of a more complex criminal scheme, this scenario illustrates how value sabotage in cybersecurity can be complemented by different forms of criminal activity to maximize the financial return for the perpetrators. In this case, money laundering was crucial for the threat actors. The attackers leveraged legitimate banking protocols to perpetrate their fraud. Besides the usual reputational damage, the action exposed systemic flaws in the global financial servicescape.

Malicious insiders: In October 2024, a Disney employee who had been recently fired due to misconduct breached the company's networks and altered the contents of the restaurant menus (Towfighi, 2024). He also utilized a bot to attempt logins on behalf of at least 14 Disney employees, resulting in their accounts being locked. Despite his previous termination, the former employee still had access to his corporate credentials, which he used to perpetrate the malicious act, motivated by a desire of revenge. In April 2025, he was sentenced to 3 years in prison and a fine of 690,000 USD (Towfighi, 2024). According to analysts, this case epitomizes the destructive impact that malicious insiders can have on organizational networks, due to their privileged access, motivation and potential to go unnoticed for long periods (Homoliak *et al*., 2019; Saxena *et al*., 2020). Besides specific services and products marketed by suppliers to protect organizations from malicious insiders, governments regularly publish defensive guidelines to tackle this specific threat.

Mechanisms of value sabotage: This scenario illustrates value sabotage dynamics similar to those involving *hacktivists*, in particular, the Randall Schwartz scenario we illustrated before. As in that case, malicious insiders exploit their intimate knowledge of the systems and flaws of the target organization. Malicious insiders epitomize the dynamics associated with sabotaging. The word "sabotage" derives from French *sabot*, indicating a wooden shoe or clog often worn by industrial workers and likely associated with intentional work performance disruptions as a form of protest (https://www.merriam-webster.com/dictionary/sabotage). Disgruntled employees are a typical category of malicious insiders.

5. Discussion

Through our taxonomy of cyber-attackers and their varying impacts on the CSaaS ecosystem, we have proposed a model that illustrates the critical role that adversaries play in driving value co-creation and service exchange between suppliers and consumers (organizations) in B2B CSaaS, through value sabotage and its varying mechanisms. Based on the existing service and cybersecurity literature, we argue that attackers act as a social force in the ecosystem. Drawing from our examples, we synthesize how attackers impact value co-creation and service exchange in CSaaS. This aligns with service management literature on service innovation (Kowalkowski *et al*., 2024). Our work also contributes to the growing literature on digital service platforms, showing how cybersecurity ecosystems operate not just through human relationships but through technology-mediated touchpoints where value and risk circulate simultaneously (Breidbach *et al*., 2014). This dual flow of value and threat distinguishes cybersecurity services from many traditional service settings.

Recent IS research reinforces the view that cybersecurity risks emerge from the structural complexity of interorganizational systems rather than isolated technical failures. For instance, Liang *et al*. (2025) demonstrate that mergers and acquisitions significantly increase data breaches due to heightened system complexity and institutional misalignment. Their findings illustrate how interconnected organizational and technological configurations create new attack surfaces, aligning with our argument that adversarial activity is an emergent force embedded in the socio-technical fabric of digital service ecosystems. In a similar vein, Tanriverdi *et al*. (2025) distinguish between organizational complexity and complicatedness,

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

showing that ad hoc, nonlinear interactions across socio-technical systems exacerbate cybersecurity breaches. Their findings complement our framework by illustrating that adversarial vulnerabilities are embedded in the structural design and interdependence of service systems rather than isolated technical failures.

CSaaS functions as a digitally mediated platform ecosystem where value exchange, governance and coordination rely on multi-actor institutional arrangements. Foundational research has emphasized how service ecosystems are shaped through complex actor interactions, resource integration and institutional structures (Akaka *et al.*, 2013; Chandler and Vargo, 2011). Building on this, recent scholarship highlights how digital ecosystems are driven not only by providers and consumers but also by orchestrators and intermediaries who manage resource flows and enable seamless service (Breidbach *et al.*, 2016; Kohtamäki *et al.*, 2019). Moreover, the evolving literature on co-creation emphasizes that value is created interactively across actors, technologies and platforms (Ramaswamy and Ozcan, 2018), advancing the service-dominant logic perspective (Lusch and Vargo, 2014). Our work extends these conversations, showing how adversarial actors disrupt not just bilateral relationships but the broader institutional and governance structures of the ecosystem (e.g., the case of hackers acting as institutional entrepreneurs that work in reconfiguring value propositions and associated governance arrangements), forcing continuous adaptation, defensive innovation and resilience-building within digitally mediated environments like CSaaS.

To capture the intentional nature of cyber-attackers' actions in disrupting the value that is exchanged in the cybersecurity service ecosystem, we propose the novel concept of "value sabotage," which we define as a *deliberate act by a social force (in our case, cyber-attackers) aimed at undermining, disrupting or degrading the value creation processes within a service ecosystem*. We argue that this necessary definition complements the concept of value co-destruction, addressing the specificity of intentionality in cyber-attackers' actions. As attackers' skills and sophistication increase (CrowdStrike, 2023), the likelihood of an organization suffering a damaging attack also increases. Hence, there is greater impetus to improve or adapt CSaaS to ensure better protection for organizations or stakeholders. In our example of the Lazarus Group hacking of the Bangladesh Central Bank, the resulting financial cost exceeded 80 million USD (BBC, 2021). Although the attack was partially thwarted thanks to timely detection, the breach still caused major disruption, demonstrating the scale and danger of coordinated cyber-attacks. In response to the impact of such attacks, organizations demand more and timelier, information about the evolving cyber-threat landscape (Bromiley, 2016). Cybersecurity suppliers and MSSPs need to keep pace with such demands to stay competitive. Against this backdrop, collaboration between suppliers and consumers is essential. Cyber threat intelligence is built exactly around this type of collaboration. MSSPs sell cyber threat intelligence to their client organizations. Besides money, the latter also contribute additional threat intelligence to the former by, for example, sharing information about threats they observe in their own environment. This leads to a value co-creation process that improves the overall quality of available threat intelligence.

As for hacktivists, the Randall Schwartz case was one of the first drivers toward the creation of bug bounty programs. Such programs are aimed at redirecting attackers' efforts and allowing them to contribute to the value co-creation process by empowering their detection of "bugs" or vulnerabilities within an organization and using their findings to improve protections.

However, value co-creation in CSaaS is not always for the benefit of client organizations. In some instances, suppliers innovate to protect themselves. In the Mondelez vs Zurich case study, cyber-insurers were wary of providing coverage for alleged *acts of war* (Ferland, 2019). Largely driven by the level of skill and dedication of state-nexus actors, leading to complexities for insurers delivering coverage, acts of war are excluded from cyber-insurance coverage. With this exclusion, the cyber-insurance industry has shifted part of the responsibility for cybersecurity back to client organizations. This indicates the capacity of state-nexus actors to indirectly impact the CSaaS ecosystem through value sabotage.

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

5.1 Mechanisms underlying value sabotage

Our six illustrative scenarios have exemplified the specifics of the mechanisms that unfold against the backdrop of value sabotage. They present significant commonalities as well as nuances that epitomize the complexity of value sabotage as a new theoretical construct in the service management literature. The illustrative scenarios we have presented are not intended to be exhaustive, but it is important to synthesize here what they "teach us" about mechanisms for value sabotage and how value sabotage differs from value co-destruction.

First, value sabotage can result from direct action by adversaries who target a specific organization (e.g. the NSO Group case) or from indirect operations that deliberately destroy value (e.g. the NotPetya case). Second, the range of motivations behind value sabotage is that typical of cyber-attackers: financial gain (e.g. the Lazarus group case), political/geopolitical motives (e.g. the NotPetya case), visibility (e.g. the TalkTalk case), etc. Third, the scope and impact of value sabotage can range from focused (e.g. the Disney case) to systemic (e.g. the NotPetya case). Fourth, the nature of value sabotage can be covert (e.g. the NSO Group case) or overt (e.g. the TalkTalk case). Fifth, value sabotage can manifest as an open violation of existing legislation (e.g. the Lazarus group case) or leverage "gray" legislative areas where the concept of ethics takes a prominent role (e.g. the Randall Schwartz case). Last, once publicized, value sabotage almost always results in reputational damage for the affected organizations when the sabotage brings to light their shortcomings or weaknesses (e.g. the Randall Schwartz or the NSO Group cases).

Our conceptual framework has also demonstrated that the mechanisms of value sabotage depend more on the context in which they unfold than on the type of adversaries that are behind them. For example, one cannot conclude that state-nexus actors always perpetrate indirect value sabotage, as in the NotPetya case: state-nexus actors can well decide to directly target an organization, thereby perpetrating a direct type of value sabotage. From this, we can draw an important methodological consideration for further investigations of value sabotage in service management literature: given the limited maturity of this field and the high dependence on context, researchers should first further explore value sabotage by adopting qualitative methods (e.g. case studies), which suit the influence that context has on the investigated constructs.

We have mentioned that the main difference between value sabotage and value co-destruction stems from the intentionality that characterizes the former. From this, a series of considerations can be drawn that further elicit the differences between these two ill-explored constructs in the service management literature. Table 3 offers a more complete overview of such differences.

A comparison between value sabotage and value co-destruction being ancillary to the core focus of the present research, we recommend future investigations to more directly focus on contrasting these two nascent constructs in the service management literature, across different industries.

Table 3. Value sabotage and value co-destruction: a comparative table

	Value sabotage	Value co-destruction
Intentionality	Intentional actions differently motivated (financial gain, visibility, etc.)	Unintentional, emerging and often driven by misalignment
Main actors	Adversaries, internal or external	Service actors (suppliers, consumers)
Trigger	Exploitation of vulnerabilities, infiltration, 'brute force'	Miscommunication, lack of coordination, unmet expectations
Response	Defensive innovation, resilience-building	Service re-design

Source(s): Authors' own work

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

5.2 Generalizability to other industries

Our conceptual framework demonstrates the role that different types of attackers have in shaping the CSaaS ecosystem through value sabotage. As a social force (Edvardsson *et al.*, 2011) in constant interaction with service providers (cybersecurity service suppliers) and service consumers (organizations), attackers play a vital role in "making the ecosystem move" and, often, triggering innovation. This aligns with the broader view in service ecosystem research, where engagement platforms create the touchpoints through which actors interact and co-create value (Breidbach *et al.*, 2014). In this sense, cybersecurity is quite a unique industry, but not the only one. For example, in the physical security industry, service providers (e.g. law enforcement or private security firms) must continuously adapt their offerings based on the evolving tactics of adversaries (e.g. criminals or protestors). This reflects the triadic interplay of supplier, consumer and attacker, as illustrated in our framework. Similarly, in financial services, institutions face threats from fraudsters motivated by economic gains. This influences the design and delivery of anti-fraud and, in general, risk management services. Even in healthcare, adversarial actors such as data thieves or ransomware groups influence the development of patient data protection services. As a result, service providers adapt their service strategies accordingly. This explains, for example, the emphasis on protecting personally identifiable information (PII) in healthcare. The above examples reinforce the relevance of our value sabotage framework across diverse service ecosystems.

More generally, the notion of an adversarial third party can also bear similarities to instances of corporate/industrial espionage or other aggressive ethically grey actions undertaken by a competitor (Sinha, 2012). A particularly aggressive competitor can, in some scenarios, act in a way to undermine an organization's ability to deliver services. For example, NDS Group, a provider of pay-TV encryption technology, was allegedly involved in espionage against Canal+, enabling unauthorized access to its subscription content and undermining its revenue model (Crane, 2005). If we hypothesize the creation of a security service to prevent NDS's actions, the triadic model proposed in our framework would also apply.

5.3 Beyond a triadic model?

The case studies illustrated in the present paper have also highlighted that the proposed triadic model could simply be a starting point. Besides value sabotage, other social forces could be in action in value co-creation and service exchange in CSaaS. Two examples of such additional forces are **regulators** and **end-customers**.

As demonstrated in vast literature, compliance with regulations is a significant driver in the cybersecurity industry (Gale *et al.*, 2022): demand-side organizations purchase cybersecurity services to avoid regulatory fines, sanctioning lax security practices and ill-advised attempts to protect consumers' data. In response, suppliers adapt their services to support organizations in their compliance efforts. An example of this is the rise of external auditing services, in which organizations voluntarily undergo assessments to prevent non-compliance with cyber-regulations.

Another significant social force is end-customers, who can drive organizations' adoption of cybersecurity best practices based on the sensitivity of the shared information, the involved assets (e.g. banking services) and a general willingness to be "protected" by the companies they do business with. Often, end-customers' data are the real target of cyber-attackers, who are aware of the reputational and financial implications associated with suboptimal practices in privacy protection. This is certainly the case with ransomware attacks (Moller, 2023). Figure 2 constitutes an evolution of the triadic model, accounting for the roles of regulators and end-customers as additional social forces.

Further research is required in this space. However, increased security demands from end-customers could lead to the evolution of the B2C cybersecurity market or the increase in B2B2C offerings, where suppliers provide security services to organizations for the direct security benefit of their end-customers.

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

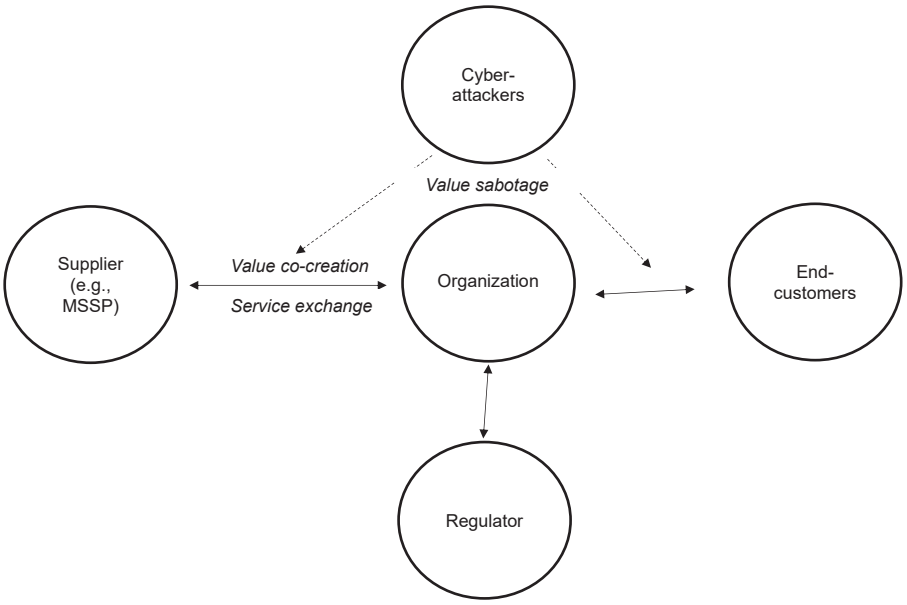

Figure 2. Pentadic model for CSaaS. Source: Authors' own work

6. Conclusion

In the present paper, through an extensive literature review and the use of six prominent case studies, we propose a novel service ecosystem model that applies to the CSaaS ecosystem and conceptualizes value sabotage as the impact that cyber-attackers have on the ecosystem. We highlight the role of cyber-attackers as a social force that influences value co-creation and service exchange in CSaaS through value sabotage. Despite being rare, a triadic framework for service production and consumption is characteristic not only of cybersecurity but of the security industry in general, where the actions of attackers are determinant in shaping the servicescape. Our work recognizes adversarial actors in the service triad, with implications for other service management scenarios, including the security industry as a whole. Moreover, our work illustrates how different types of attackers may differently impact value co-creation and service exchange in CSaaS, as we depict through practical examples (e.g. cyber-insurance services, cyber threat intelligence, cybersecurity service innovation).

Our framework captures the unique complexity of the cybersecurity landscape, where external threats fundamentally influence service interactions and outcomes. Our model demonstrates that cyber-attackers are not merely disruptors (or saboteurs), but active forces orchestrating innovation, resilience and strategic adaptation in the cybersecurity sector. Their actions compel service providers and consumers to co-create value through defensive and preventative measures, highlighting a paradigm shift from traditional customer satisfaction to shared resilience against adversarial forces. We invite other researchers to empirically extend our proposed framework: an exploratory investigation of the emergent dynamics in the cybersecurity service ecosystem triggered by cyber-attackers' actions could provide further nuance to our conceptual model.

This study contributes significant insights to service literature, service innovation and service management by integrating the role of cyber-attackers into the conceptual framework of service ecosystems. Traditional service literature has predominantly focused on constructive dyadic or triadic relationships between providers, consumers and

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

intermediaries. However, cybersecurity services present a novel dynamic, where adversarial actors, such as cyber-attackers, actively disrupt and reshape value co-creation processes. Recognizing attackers as key players, this research challenges conventional perspectives and underscores the importance of addressing adversarial forces in service theories.

While prior research has examined service triads involving intermediaries or constructive collaborators, our model highlights the unique impact of adversarial forces that continuously threaten system stability. This focus advances service ecosystem theory by foregrounding the role of malicious actors as key drivers of defensive innovation, adaptive capability and institutional change, particularly within digitally mediated platforms such as CSaaS. Our work has ultimately laid the foundations for the study of two additional social forces and their influence on the CSaaS ecosystem: regulators and end-customers. Looking ahead, future research could explore how non-malicious competitors, pursuing conflicting objectives such as market leadership or innovation advantage, function as adversarial forces within service ecosystems, shaping value co-creation and co-destruction dynamics alongside more explicitly disruptive actors. Would we be talking about value sabotage in these instances, too? We invite fellow researchers to join us in investigating whether a pentadic framework best represents the dynamics that characterize the security services ecosystem.

References

Aanestad, M., Hanseth, O., Monteiro, E., Niemimaa, M. and Ribes, D. (2024), "From methodological symmetry to Gaia: Latour's legacy and untapped potential for IS research", *Journal of the Association for Information Systems*, Vol. 25 No. 2, pp. 182-195, available at: https://aisel.aisnet.org/jais/vol25/iss2/10

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L.F. and Abdulkadir, S.J. (2022), "Detecting cybersecurity attacks in internet of things using artificial intelligence methods: a systematic literature review", *Electronics*, Vol. 11 No. 2, p. 198, doi: 10.3390/electronics11020198.

Ablon, L. (2018), *The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*, RAND Corporation, Santa Monica, CA.

Abrahams, T.O., Ewuga, S.K., Dawodu, S.O., Adegbite, A.O. and Hassan, A.O. (2024), "A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection", *A Review Of Cybersecurity Strategies In Modern Organizations: Examining The Evolution And Effectiveness Of Cybersecurity Measures For Data Protection*, Vol. 5 No. 1, pp. 1-25, doi: 10.51594/csitrj.v5i1.699.

Accenture (2023), "Accenture's cyber-resilient CEO report", available at: https://newsroom.accenture.com/news/2023/ceos-lack-confidence-in-their-organizations-ability-to-protect-against-cyberattacks-despite-seeing-cybersecurity-as-vital-to-growth-accenture-report-finds (accessed 8 December 2024).

Ackerman, R. (2021), "Government and private sector cybersecurity collaboration finally showing signs of life", *RSA Conference*, available at: https://www.rsaconference.com/library/blog/government-and-private-sector-cybersecurity-collaboration-finally-showing-signs-of-life (accessed 12 December 2024).

Adriano, L. (2022), "Zurich, Mondelez settle longstanding lawsuit over $100 million claim", available at: https://www.insurancebusinessmag.com/us/news/cyber/zurich-mondelez-settle-longstanding-lawsuit-over-100-million-claim-426741.aspx (accessed 12 December 2024).

Akaka, M.A., Vargo, S.L. and Lusch, R.F. (2013), "The complexity of context: a service ecosystems approach for international marketing", *Journal of International Marketing*, Vol. 21 No. 4, pp. 1-20, doi: 10.1509/jim.13.0032.

Al Maamari, W., Ahmed, M., Said, R.B. and Marhaban, M. (2024), "Cybersecurity Incident Response Dynamics: unveiling emerging trends and confronting persistent challenges", *Computer Science and Information Technology 2024*, pp. 45-55, doi: 10.5121/csit.2024.141104.

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

Alkhadra, R., Abuzaid, J., AlShammari, M. and Mohammad, N. (2021), "Solar winds hack: in-depth analysis and countermeasures", *IEEE Xplore*, Vol. 1 July, doi: 10.1109/ICCCNT51525.2021.9579611.

Allen, J., Crabb, G., Curtis, P., Fitzpatrick, B., Mehravari, N. and Tobar, D. (2015), "Structuring the chief information officer organization", in *Software Engineering Institute*, Carnegie Mellon University, available at: https://insights.sei.cmu.edu/documents/2298/2015_004_001_446198.pdf

Almansoori, A., Al-Emran, M. and Shaalan, K. (2023), "Exploring the frontiers of cybersecurity behavior: a systematic review of studies and theories", *Applied Sciences*, Vol. 13 No. 9, p. 5700, doi: 10.3390/app13095700.

Alvarez, R. (2017), *Key Differences between Petya and NotPetya*, Fortinet Blog, 9 July, available at: https://www.fortinet.com/blog/threat-research/key-differences-between-petya-and-notpetya (accessed 12 December 2024).

Ansari, M.F., Dash, B., Sharma, P. and Yathiraju, N. (2022), "The impact and limitations of artificial intelligence in cybersecurity: a literature review", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 11 No. 9, doi: 10.17148/ijarcce.2022.11912.

Arshad, J., Talha, M., Saleem, B., Shah, Z., Zaman, H. and Muhammad, Z. (2024), "A survey of bug bounty programs in strengthening cybersecurity and privacy in the blockchain industry", *Blockchains*, Vol. 2 No. 3, pp. 195-216, doi: 10.3390/blockchains2030010.

Atrews, R.A. (2020), "Cyberwarfare: threats, security, attacks, and impact", *Journal of Information Warfare*, Vol. 19 No. 4, pp. 17-28.

August, T., Dao, D. and Niculescu, M.F. (2022), "Economics of ransomware: risk interdependence and large-scale attacks", *Management Science*, Vol. 68 No. 12, pp. 8979-9002, doi: 10.1287/mnsc.2022.4300.

BBC News (2018), *UK and US Blame Russia for 'malicious' NotPetya Cyber-Attack*, BBC News, 15 February, available at https://www.bbc.com/news/uk-politics-43062113 (accessed 5 December 2025)

BBC News (2021), *The Lazarus Heist: How North Korea Almost Pulled off a Billion-Dollar Hack*, BBC News, 20 June, available at https://www.bbc.com/news/stories-57520169 (accessed 5 December 2025).

Bijlenga, N. and Kleemans, E.R. (2018), "Criminals seeking ICT-expertise: an exploratory study of Dutch cases", *European Journal on Criminal Policy and Research*, Vol. 24 No. 3, pp. 253-268, doi: 10.1007/s10610-017-9356-z.

Bongiovanni, I., Renaud, K., Brydon, H., Blignaut, R. and Cavallo, A. (2022), "A quantification mechanism for assessing adherence to information security governance guidelines", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print, pp. 517-548, doi: 10.1108/ics-08-2021-0112.

Bordian, M., Gil-Saura, I. and Šerić, M. (2022), "The impact of value co-creation in sustainable services: understanding generational differences", *Journal of Services Marketing*, Vol. 37 No. 2, pp. 155-167, doi: 10.1108/jsm-06-2021-0234.

Breidbach, C.F. and Brodie, R.J. (2017), "Engagement platforms in the sharing economy: conceptual foundations and research directions", *Journal of Service Theory and Practice*, Vol. 27 No. 4, pp. 761-777, doi: 10.1108/jstp-04-2016-0071.

Breidbach, C.F., Brodie, R. and Hollebeek, L. (2014), "Beyond virtuality: from engagement platforms to engagement ecosystems", *Managing Service Quality*, Vol. 24 No. 6, pp. 592-611, doi: 10.1108/MSQ-08-2013-0158.

Breidbach, C.F., Antons, D. and Salge, T.O. (2016), "Seamless service? On the role and impact of service orchestrators in human-centered service systems", *Journal of Service Research*, Vol. 19 No. 4, pp. 458-476, doi: 10.1177/1094670516666370.

Bromiley, M. (2016), *Threat Intelligence: What it Is, and How to Use it Effectively*, SANS Institute, North Bethesda, MD.

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

Brooks, R.R., Ozcelik, I., Yu, L., Oakley, J. and Tusing, N. (2021), "Distributed denial of service (DDoS): a history", *IEEE Annals of the History of Computing*, Vol. 44 No. 2, p. 1, doi: 10.1109/mahc.2021.3072582.

Cai, C. and Zhang, R. (2025), "Fragmentation of global cybersecurity governance: quasi-public goods and multi-level conflicts", *Bristol University Press*, Vol. 4 No. 1, pp. 32-50, doi: 10.1332/26352257Y2024D000000016.

Cartwright, P. (2014), "Understanding and protecting vulnerable financial consumers", *Journal of Consumer Policy*, Vol. 38 No. 2, pp. 119-138, doi: 10.1007/s10603-014-9278-9.

Cayubit, R.F.O., Rebolledo, K.M., Kintanar, R.G.A., Pastores, A.G., Santiago, A.J.A. and Valles, P.B.V. (2017), "A cyber phenomenon: a Q-analysis on the motivation of computer hackers", *Psychological Studies*, Vol. 62 No. 4, pp. 386-394, doi: 10.1007/s12646-017-0423-9.

Center for Internet Security (2024), "Cybersecurity spotlight - cyber threat actors", CIS, 1 January, available at: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors (accessed 12 December 2024).

Chandler, J.D. and Vargo, S.L. (2011), "Contextualization and value-in-context: how context frames exchange", *Marketing Theory*, Vol. 11 No. 1, pp. 35-49, doi: 10.1177/1470593110393713.

Chng, S., Lu, H.Y., Kumar, A. and Yau, D. (2022), "Hacker types, motivations and strategies: a comprehensive framework", *Computers in Human Behavior Reports*, Vol. 5, 100167, doi: 10.1016/j.chbr.2022.100167.

CompaniesMarketCap (2024), "Largest IT security companies by market cap", *Companiesmarketcap.com*, available at: https://companiesmarketcap.com/aud/it-security/largest-companies-by-market-cap/ (accessed 12 December 2024).

Craig, A. and Valeriano, B. (2016), "Conceptualising cyber arms races", *2016 8th International Conference on Cyber Conflict, NATO*, pp. 141-158, doi: 10.1109/cycon.2016.7529432, available at: https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf (accessed 15 July 2025).

Crane, A. (2005), "In the company of spies: when competitive intelligence gathering becomes industrial espionage", *Business Horizons*, Vol. 48 No. 3, pp. 233-240, doi: 10.1016/j.bushor.2004.11.005.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A., Mullins, M., Murphy, F. and Materne, S. (2022), "Cyber risk and cybersecurity: a systematic review of data availability", *The Geneva Papers on Risk and Insurance - Issues and Practice*, Vol. 47 No. 3, pp. 698-736, doi: 10.1057/s41288-022-00266-6.

Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B.J. and Materne, S. (2024), "On the insurability of cyber warfare: an investigation into the German cyber insurance market", *Computers and Security*, Vol. 142, 103886, doi: 10.1016/j.cose.2024.103886.

CrowdStrike (2023), "2023 global threat report".

Cyber Security Industry Advisory Committee (2021a), *Australia's Cyber Security Strategy 2020*, Department of Home Affairs, Canberra, ACT.

Cyber Security Industry Advisory Committee (2021b), "Locked out: tackling Australia's ransomware threat cyber security industry advisory committee", Canberra, ACT.

De Bruijne, M., Van Eeten, M., Gañán, C. and Pieters, W. (2017), "Towards a new cyber threat actor typology a hybrid method for the NCSC cyber security assessment".

Department of Foreign Affairs and Trade (2021), "FAQs cyber sanctions and ransomware payments", Australian Government Department of Foreign Affairs and Trade, available at: https://www.dfat.gov.au/international-relations/security/sanctions/guidance/faqs-cyber-sanctions-and-ransomware-payments (accessed 12 December 2024).

Di Marco, B. (2023), "War exclusions in cyber policies: the important details", June, available at: https://www.wtwco.com/en-au/insights/2023/06/war-exclusions-in-cyber-policies-the-important-details (accessed 12 December 2024).

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

Dickinson, E. (2024), "MediSecure calls in administrators after cyber breach", 5 June, available at: https://www.itnews.com.au/news/medisecure-calls-in-administrators-after-cyber-breach-608580 (accessed 12 December 2024).

Ding, W., Yurcik, W. and Yin, X. (2005), "Outsourcing internet security: economic analysis of incentives for managed security service providers", in *International Workshop on Internet and Network Economics*, Springer, pp. 947-958, doi: 10.1007/11600930_96.

Dupuis, M. and Khadeer, S. (2016), "Curiosity killed the organization: a psychological comparison between malicious and non-malicious insiders and the insider threat", *Proceedings of the 5th Annual Conference on Research in Information Technology*, pp. 35-40, doi: 10.1145/2978178.2978185.

Edvardsson, B., Tronvoll, B. and Gruber, T. (2011), "Expanding understanding of service exchange and value co-creation: a social construction approach", *Journal of the Academy of Marketing Science*, Vol. 39 No. 2, pp. 327-339, doi: 10.1007/s11747-010-0200-y.

ENISA (2024), "ENISA threat landscape 2024", ENISA, October, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

EY (2020), "EY global information security survey 2020, EY".

Fehrer, J.A., Woratschek, H., Germelmann, C.C. and Brodie, R.J. (2018), "Dynamics and drivers of customer engagement: within the dyad and beyond", *Journal of Service Management*, Vol. 29 No. 3, pp. 443-467, doi: 10.1108/josm-08-2016-0236.

Feng, N., Wang, M., Li, M. and Li, D. (2019), "Effect of security investment strategy on the business value of managed security service providers", *Electronic Commerce Research and Applications*, Vol. 35, 100843, doi: 10.1016/j.elerap.2019.100843.

Ferland, J. (2019), "Cyber insurance–What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case", *Computer Law and Security Review*, Vol. 35 No. 4, pp. 369-376, doi: 10.1016/j.clsr.2019.06.003.

Gale, M., Bongiovanni, I. and Slapničar, S. (2022), "Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead", *Computers and Security*, Vol. 121 No. 1, 102840, doi: 10.1016/j.cose.2022.102840.

Greenberg, A. (2018), "The untold story of NotPetya, the most devastating cyberattack in history", *WIRED, Condé Nast*, 22 August, available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Gulyas, O. and Kiss, G. (2023), "Impact of cyber-attacks on the financial institutions", *Procedia Computer Science*, Vol. 219, pp. 84-90, doi: 10.1016/j.procs.2023.01.267.

HackerOne (2021), "What is a bug bounty? Should you offer one? And how to do it", *HackerOne*, 9 November, available at: https://www.hackerone.com/vulnerability-management/what-bug-bounty-should-you-offer-one-and-how-do-it (accessed 12 December 2024).

Hald, S.L.N. and Pedersen, J.M. (2012), "An updated taxonomy for characterising hackers according to their threat properties", *2012 14th International Conference on Advanced Communication Technology (ICACT)*, IEEE, pp. 81-86.

Harrmann, L.K., Eggert, A. and Böhm, E. (2022), "Digital technology usage as a driver of servitization paths in manufacturing industries", *European Journal of Marketing*, Vol. 57 No. 3, pp. 834-857, doi: 10.1108/ejm-11-2021-0914.

Heino, J., Hakkala, A. and Virtanen, S. (2022), "Study of methods for endpoint aware inspection in a next generation firewall", *Cybersecurity*, Vol. 5 No. 1, 25, doi: 10.1186/s42400-022-00127-8.

Hepfer, M. and Powell, T.C. (2020), "Make cybersecurity a strategic asset", *MIT Sloan Management Review*, Vol. 62 No. 1, pp. 40-45, available at: https://uoelibrary.idm.oclc.org/login?url=https://www.proquest.com/scholarly-journals/make-cybersecurity-strategic-asset/docview/2450655586/se-2.

Hern, A. (2016), "TalkTalk hit with record £400k fine over cyber-attack", The Guardian, The Guardian, 5 October, available at: https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack (accessed 12 December 2024).

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

Hern, A. (2017a), "Major cyber-attack will happen soon, warns UK's security boss", *The Guardian*, 22 September.

Hern, A. (2017b), "WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017", The Guardian, The Guardian, 30 December, available at: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware (accessed 12 December 2024).

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. and Ochoa, M. (2019), "Insight into insiders and it: a survey of insider threat taxonomies, analysis, modeling, and countermeasures", *ACM Computing Surveys*, Vol. 52 No. 2, pp. 1-40, doi: 10.1145/3303771.

Hopkins, N. and Kirchgaessner, S. (2019), "WhatsApp sues Israeli firm, accusing it of hacking activists' phones", *The Guardian*, 29 October.

Huang, K., Siegel, M. and Madnick, S. (2017), "Cybercrime-as-a-service: identifying control points to disrupt", *Massachusetts Institute of Technology (MIT), Tech. Rep*.

ICO (2016), "TalkTalk cyber attack – how the ICO's investigation unfolded", available at: https://ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/

Jeffrey, D. (2024), "Half of all Australians hit by MediSecure hack, but company can't afford to find out who", 18 July, available at: https://www.9news.com.au/national/medisecure-hack-12-9-million-australians-affected/3c44cd81-b1c4-482c-9007-67f50a90f04f (accessed 12 December 2024).

Kabir, M. (2023), "Lessons learned from the Bangladesh Bank heist", ISACA, available at: https://www.isaca.org/resources/isaca-journal/issues/2023/volume-6/lessons-learned-from-the-bangladesh-bank-heist

Kaspersky (2023), "Redefining the human factor in cybersecurity", available at: https://www.kaspersky.com/blog/human-factor-360-report-2023 (accessed 11 December 2024).

Kirchgaessner, S. (2024a), "NSO – not government clients – operates its spyware, legal documents reveal", *The Guardian*, The Guardian, 15 November, available at: https://www.theguardian.com/technology/2024/nov/14/nso-pegasus-spyware-whatsapp (accessed 12 December 2024).

Kirchgaessner, S. (2024b), "Court orders maker of Pegasus spyware to hand over code to WhatsApp", *The Guardian*, 29 February.

Kohtamäki, M., Parida, V., Oghazi, P., Gebauer, H. and Baines, T. (2019), "Digital servitization business models in ecosystems: a theory of the firm", *Journal of business research*, Vol. 104, pp. 380-392, doi: 10.1016/j.jbusres.2019.06.027.

Konyeha, S. (2020), "Exploring cybersecurity threats in digital marketing", *NIPES Journal of Science and Technology Research*, Vol. 2 No. 3, p. 12, doi: 10.37933/nipes/2.3.2020.2.

Kowalkowski, C., Wirtz, J. and Ehret, M. (2024), "Digital service innovation in B2B markets", *Journal of Service Management*, Vol. 35 No. 2, pp. 280-305, doi: 10.1108/JOSM-12-2022-0403.

KPMG (2021), "The changing shape of ransomware".

Lewis, P.H. (1995), "Technology: on the net; An Intel computer security expert runs afoul of the law. So much for the 'hacker ethic'? (Published 1995)", *The New York Times*.

Li, Y. and Liu, Q. (2021), "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments", *Energy Reports*, Vol. 7 No. 7, pp. 8176-8186, doi: 10.1016/j.egyr.2021.08.126.

Liang, H., Srinivas, S. and Xue, Y. (2025), "How mergers and acquisitions increase data breaches: a complexity perspective", *MIS Quarterly*, Vol. 49 No. 1, pp. 211-242, doi: 10.25300/MISQ/2023/17703.

Lumivalo, J., Tuunanen, T. and Salo, M. (2024), "Value co-destruction: a conceptual review and future research agenda", *Journal of Service Research*, Vol. 27 No. 2, pp. 159-176, doi: 10.1177/10946705231177504.

Lusch, R.F. and Nambisan, S. (2015), "Service innovation", *MIS Quarterly*, Vol. 39 No. 1, pp. 155-176, available at: https://www.jstor.org/stable/26628345

Lusch, R.F. and Vargo, S.L. (2014), *The Service-Dominant Logic of Marketing: Dialog, Debate, and Directions*, Routledge, London.

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

Malatji, M. and Tolah, A. (2025), "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI", *AI and Ethics*, Vol. 5 No. 2, pp. 883-910, doi: 10.1007/s43681-024-00427-4.

Malhotra, A. and Kubowicz Malhotra, C. (2011), "Evaluating customer information breaches as service failures: an event study approach", *Journal of Service Research*, Vol. 14 No. 1, pp. 44-59, doi: 10.1177/1094670510383409.

Mark, C. (2024), "Understanding cyber attacker motivations to best apply controls", 6 January, available at: https://levelblue.com/blogs/security-essentials/understanding-cyber-attacker-motivations-to-best-apply-controls

Mascellino, A. (2022), "Zurich and Mondelez reach NotPetya settlement, but cyber-risk may increase", *Infosecurity Magazine*, 3 November, available at: https://www.infosecurity-magazine.com/news/notpetya-settlement-may-increase/ (accessed 12 December 2024).

McCombie, S. (2018), "Threat actor oriented strategy: knowing your enemy to better defend, detect and respond to cyber-attacks", *Journal of the Australian Institute of Professional Intelligence Officers*, Vol. 26 No. 1, pp. 24-41.

Meland, P.H., Bayoumy, Y.F.F. and Sindre, G. (2020), "The Ransomware-as-a-Service economy within the darknet", *Computers and Security*, Vol. 92 No. 1, 101762, doi: 10.1016/j.cose.2020.101762.

Minaya, P.E., Avella, L. and Trespalacios, J.A. (2024), "Synthesizing three decades of digital servitization: a systematic literature review and conceptual framework proposal", *Service Business*, Vol. 18 No. 2, pp. 193-222, doi: 10.1007/s11628-024-00559-x.

MITRE (2024), "Mitre ATT&CK™", available at: https://attack.mitre.org/

Moller, D.P. (2023), "Ransomware attacks and scenarios: cost factors and loss of reputation", *Guide to Cybersecurity in Digital Transformation*, pp. 273-303, doi: 10.1007/978-3-031-26845-8_6.

Mordor Intelligence (2025), "Cyber security market size, shares, trends & industry (2025-2030)", *Mordo Intelligence*, available at: https://www.mordorintelligence.com/industry-reports/cyber-security-market

Morris, J., Tatschner, S., Heinl, M.P., Newe, T. and Plaga, S. (2023), "Cybersecurity as a service", in *Cybersecurity Vigilance and Security Engineering of Internet of Everything*, Springer Nature Switzerland, Cham, pp. 141-161, Switzerland.

Mott, G., Turner, S., Nurse, J.R.C., MacColl, J., Sullivan, J., Cartwright, A. and Cartwright, E. (2023), "Between a rock and a hard(ening) place: cyber insurance in the ransomware era", *Computers and Security*, Vol. 128 No. 1, 103162, doi: 10.1016/j.cose.2023.103162.

Naseer, H., Desouza, K., Maynard, S.B. and Ahmad, A. (2024), "Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics", *European Journal of Information Systems*, Vol. 33 No. 2, pp. 200-220, doi: 10.1080/0960085X.2023.2257168.

Ng, I.C. and Wakenshaw, S.Y. (2017), "The Internet-of-Things: review and research directions", *International Journal of Research in Marketing*, Vol. 34 No. 1, pp. 3-21, doi: 10.1016/j.ijresmar.2016.11.003.

O'Grady, J. and Malone, K. (2022), "A SWIFT getaway: planet money", NPR.org.

Paganini, P. (2024), "Slim CD disclosed a data breach impacting 1.7M individuals", Security Affairs, 10 September, available at: https://securityaffairs.com/168229/data-breach/slim-cd-disclosed-a-data-breach.html (accessed 11 December 2024).

Palma, B. (2024), "AI is transforming cybersecurity: how can security experts respond?", World Economic Forum, available at: https://www.weforum.org/stories/2024/01/arms-race-cybersecurity-ai/ (accessed 15 July 2025).

Panagiotopoulos, V. (2024), "Notorious spyware maker NSO group is quietly plotting a comeback", *Wired*, available at: https://www.wired.com/story/nso-group-lobbying-israel-hamas-war/.

Pienta, D., Thatcher, J.B., Wright, R.T. and Roth, P.L. (2024), "An empirical investigation of the unintended consequences of vulnerability assessments leading to betrayal", *Journal of the Association for Information Systems*, Vol. 25 No. 4, pp. 1079-1116, available at: https://aisel.aisnet.org/jais/vol25/iss4/2

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

Pigola, A. and de Souza Meirelles, F. (2024), "Unraveling trust management in cybersecurity: insights from a systematic literature review", *Information Technology and Management*, Vol. 1 No. 3, doi: 10.1007/s10799-024-00438-x.

Plé, L. and Chumpitaz Cáceres, R. (2010), "Not always co-creation: introducing interactional co-destruction of value in service-dominant logic", *Journal of Services Marketing*, Vol. 24 No. 6, pp. 430-437, doi: 10.1108/08876041011072546.

Poireault, K. (2023), "What have we learned from cyberattack NotPetya six years on?", 11 July, available at: https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/learnings-from-notpetya-cyberattack.html (accessed 12 December 2024).

Press Association (2016), "Teenager who hacked TalkTalk website given rehabilitation order", *The Guardian*, 13 December, available at: https://www.theguardian.com/business/2016/dec/13/teenager-who-hacked-talktalk-website-given-rehabilitation-order (accessed 12 December 2024).

PwC (2017), "Protect.me: how consumers see cyber security and privacy risks", PwC, available at: https://www.pwc.com.au/digitalpulse/report-protect-me-consumers-cyber-security.html (accessed 12 December 2024).

Ramaswamy, V. and Ozcan, K. (2018), "What is co-creation? An interactional creation framework and its implications for value creation", *Journal of Business Research*, Vol. 84, pp. 196-205, doi: 10.1016/j.jbusres.2017.11.027.

Reed, E. and Scott, K. (2017), "You may Be able to outsource privacy and cybersecurity functions, but you can't outsource the risk of liability", *Commercial Law*, Vol. 33 No. 4, pp. 4-8.

Reeder, J.R. and Hall, T. (2021), "Cybersecurity's pearl harbor moment: lessons learned from the colonial pipeline ransomware attack", *The Cyber Defense Review*, Vol. 6 No. 3, pp. 15-40.

Reeves, M. and Job, A. (2023), "The Future 50: companies built for growth in uncertain times", *Fortune*, Vol. 4 December, available at: https://fortune.com/2023/12/04/fortune-future-50-index-2023-vitality-growth-china-mercadolibre-doordash-spotify/ (accessed 12 December 2024).

Reina, N.J. (2024), "The new face of cyber threats—AI, deepfakes, and scams", Norton, 22 October, available at: https://au.norton.com/blog/emerging-threats/threat-report-q2-2024.

Rosenbaum, M.S. and Massiah, C. (2011), "An expanded servicescape perspective", *Journal of Service Management*, Fisk, R.P. (Ed.), Vol. 22 No. 4, pp. 471-490, doi: 10.1108/09564231111155088.

Roy, S.K., Singh, G., Hope, M., Nguyen, B. and Harrigan, P. (2022), "The rise of smart consumers: role of smart servicescape and smart consumer experience co-creation", *The Role of Smart Technologies in Decision Making*, pp. 114-147, doi: 10.4324/9781003307105-6.

Rundle, J. (2024), "The AI effect: Amazon sees nearly 1 billion cyber threats a day", *The Wall Street Journal*, available at: https://www.wsj.com/articles/the-ai-effect-amazon-sees-nearly-1-billion-cyber-threats-a-day-15434edd (accessed 15 July 2025).

Saha, V., Goyal, P. and Jebarajakirthy, C. (2021), "Value co-creation: a review of literature and future research agenda", *Journal of Business and Industrial Marketing*, Vols ahead-of-print Nos ahead-of-print, pp. 612-628, doi: 10.1108/jbim-01-2020-0017.

Sailio, M., Latvala, O.-M. and Szanto, A. (2020), "Cyber threat actors for the factory of the future", *Applied Sciences*, Vol. 10 No. 12, p. 4334, doi: 10.3390/app10124334.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K.R. and Burnap, P. (2020), "Impact and key challenges of insider threats on organizations and critical businesses", *Electronics*, Vol. 9 No. 9, p. 1460, doi: 10.3390/electronics9091460.

Schwartz, J. (1997), "The case of the Intel 'hacker,' victim of his own access", Washington Post, 15 September.

Scroxton, A. (2022), "Austrian data firm accused of selling malware, conducting cyber attacks", *ComputerWeekly.com*, available at: https://www.computerweekly.com/news/252523308/Austrian-data-firm-accused-of-selling-malware-conducting-cyber-attacks (accessed 12 December 2024).

Shirer, M. (2023), "New IDC spending guide forecasts worldwide security investments will grow 12.1% in 2023 to $219 billion", IDC: The Premier Global Market Intelligence Company,

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

available at: https://www.idc.com/getdoc.jsp?containerId=prUS50498423 (accessed 12 December 2024).

Sinha, S. (2012), "Understanding industrial espionage for greater technological and economic security", *IEEE Potentials*, Vol. 31 No. 3, pp. 37-41, doi: 10.1109/mpot.2012.2187118.

Slapničar, S., Axelsen, M., Bongiovanni, I. and Stockdale, D. (2023), "A pathway model to five lines of accountability in cybersecurity governance", *International Journal of Accounting Information Systems*, Vol. 51, 100642, doi: 10.1016/j.accinf.2023.100642.

Smalley, S. (2022), "Insurance giant settles NotPetya lawsuit, signaling cyber insurance shakeup", *CyberScoop*, 4 November, available at: https://cyberscoop.com/insurance-giant-settles-notpetya-lawsuit/

Smith, F. and Ingram, G. (2017), "Organising cyber security in Australia and beyond", *Australian Journal of International Affairs*, Vol. 71 No. 6, pp. 642-660, doi: 10.1080/10357718.2017.1320972.

Snider, K.L.G., Shandler, R., Zandani, S. and Canetti, D. (2021), "Cyberattacks, cyber threats, and attitudes toward cybersecurity policies", *Journal of Cybersecurity*, Vol. 7 No. 1, doi: 10.1093/cybsec/tyab019.

Sophos (2024), "Ransomware payments increase 500% in the last year, finds sophos state of ransomware report | sophos", 30 April, available at: https://www.sophos.com/en-us/press/press-releases/2024/04/ransomware-payments-increase-500-last-year-finds-sophos-state (accessed 13 December 2024).

Statista (2024), "Top cybersecurity companies worldwide by market cap 2024 | Statista", Statista, available at: https://www.statista.com/statistics/1459863/most-important-firms-cybersecurity-worldwide-by-market-cap/ (accessed 12 December 2024).

Statista (2025), "Estimated cost of cybercrime worldwide 2018-2029 | Statista", Statista, available at: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide (accessed 16 July 2025).

Stiennon, R. (2020), "The demise of symantec", *Forbes*, available at: https://www.forbes.com/sites/richardstiennon/2020/03/16/the-demise-of-symantec/

Strategy of Security (2022), "An intro to consolidation and aggregation in cybersecurity", *Strategy of Security*, available at: https://strategyofsecurity.com/p/an-intro-to-consolidation-and-aggregation-in-cybersecurity

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y. and Zhang, J. (2023), "Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives", *IEEE Communications Surveys and Tutorials*, Vol. 25 No. 3, p. 1, doi: 10.1109/comst.2023.3273282.

Tanriverdi, H., Kwon, J. and Im, G. (2025), "Taming complexity in the cybersecurity of multihospital systems: the role of enterprise-wide data analytics platforms", *MIS Quarterly*, Vol. 49 No. 1, pp. 243-274, doi: 10.25300/MISQ/2024/17752.

Temple-Raston, D. (2022), "Lapsus$: the script kiddies are alright", Therecord.media, available at: https://therecord.media/lapsus-the-script-kiddies-are-alright

Tiberius, V., Rietz, M. and Bouncken, R.B. (2020), "Performance analysis and science mapping of institutional entrepreneurship", *Administrative Sciences*, Vol. 10 No. 3, pp. 1-21, doi: 10.3390/admsci10030069.

Towfighi, J. (2024), "Fired Disney employee allegedly hacked into company system to change allergen info on menus", CNN, available at: https://edition.cnn.com/2024/10/30/business/fired-disney-employee-allegedly-hacked-into-company-system-to-change-allergy-info-on-menus/index.html

TrendMicro (2015), "TalkTalk reports breach, up to 4 million unencrypted records stolen - security news", available at: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/talktalk-breach-up-to-4-million-unencrypted-records-stolen (accessed 12 December 2024).

Trim, P.R.J. and Lee, Y.-I. (2019), "The role of B2B marketers in increasing cyber security awareness and influencing behavioural change", *Industrial Marketing Management*, Vol. 83, pp. 224-238, doi: 10.1016/j.indmarman.2019.04.003.

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on

US Cybersecurity and Infrastructure Security Agency (2018), "Petya ransomware | CISA", available at: https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware (accessed 15 February).

Vargo, S.L. and Lusch, R.F. (2016), "Institutions and axioms: an extension and update of service-dominant logic", *Journal of the Academy of Marketing Science*, Vol. 44 No. 1, pp. 5-23, doi: 10.1007/s11747-015-0456-3.

Villalón-Fonseca, R. (2022), "The nature of security: a conceptual framework for integral-comprehensive modeling of IT security and cybersecurity", *Computers and Security*, Vol. 120 No. 1, 102805, doi: 10.1016/j.cose.2022.102805.

Virlée, J.B., Hammedi, W. and van Riel, A.C.R. (2020), "Healthcare service users as resource integrators: investigating factors influencing the co-creation of value at individual, dyadic and systemic levels", *Journal of Service Theory and Practice*, Vol. 30 No. 3, pp. 277-306, doi: 10.1108/jstp-07-2019-0154.

Walker, D.D., Kim, S.K., van Jaarsveld, D.D., Restubog, S.L.D., Marrone, M., Lagios, C. and Mehdipour, A.M. (2023), "It takes two to tango: a multidisciplinary bibliometric review across six decades of dyadic service encounter research", *Journal of Service Management*, Vol. 34 No. 5, pp. 970-994, doi: 10.1108/josm-08-2022-0286.

Wan, K. (2020), "NotPetya, not warfare: rethinking the insurance war exclusion in NotPetya, not warfare: rethinking the insurance war exclusion in the context of international cyberattacks", *Washington Law Review Washington Law Review*, Vol. 95 No. 3, pp. 1595-1620.

Wang, X.-S., Herwono, I., Cerbo, F.D., Kearney, P. and Shackleton, M. (2018), "Enabling cyber security data sharing for large-scale enterprises using managed security services", *IEEE Xplore*, Vol. 1 May, pp. 1-7, doi: 10.1109/CNS.2018.8433212.

Wang, E.Q., Fehrer, J.A., Li, L.P., Brodie, R.J. and Juric, B. (2023), "The nature of actor engagement intensity: a classification scheme", *Journal of Service Management*, Vol. 34 No. 4, pp. 631-656, doi: 10.1108/josm-11-2022-0348.

Westendorf, T. (2021), "Pegasus spyware and the direction of Australian policing", The Strategist, 23 November, available at: https://www.aspistrategist.org.au/pegasus-spyware-and-the-direction-of-australian-policing/

Wu, Y., Feng, G., Wang, N. and Liang, H. (2015), "Game of information security investment: impact of attack types and network vulnerability", *Expert Systems with Applications*, Vol. 42 No. 15, pp. 6132-6146, doi: 10.1016/j.eswa.2015.03.033.

Zhang, L. and Thing, V.L.L. (2021), "Three decades of deception techniques in active cyber defense - retrospect and outlook", *Computers and Security*, Vol. 106 No. 1, 102288, doi: 10.1016/j.cose.2021.102288.

Zhang, L., Demirezen, E.M. and Kumar, S. (2024), "How to make my bug bounty cost-effective? A game-theoretical model", *SSRN Electronic Journal*, Vol. 36 No. 2, pp. 1031-1053, doi: 10.2139/ssrn.4869779.

Zrahia, A. (2018), "Threat intelligence sharing between cybersecurity vendors: network, dyadic, and agent views", *Journal of Cybersecurity*, Vol. 4 No. 1, tyy008, doi: 10.1093/cybsec/tyy008.

Further reading

Australian Signals Directorate (2023), "Annual Cyber Threat Report 2023-2024 | Cyber.gov.au", available at: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024?utm_source=email&utm_medium=stakeholder_toolkit&utm_campaign=ACTR2024 (accessed 12 December 2024).

Australia's Cyber (n.d.), "Security strategy 2020—cyber security industry advisory committee annual report 2021".

Corresponding author
Ivano Bongiovanni can be contacted at: i.bongiovanni@uq.edu.au

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**

Downloaded from http://ftp.nowpublishers.com/josm/article-pdf/doi/10.1108/JOSM-12-2024-0537/11001915/josm-12-2024-0537en.pdf by guest on