www.itcon.org - Journal of Information Technology in Construction - ISSN 1874-4753

PATHWAYS TO CYBER PERIL: TEN CONFIGURATIONAL ROUTES TO CYBERSECURITY BREACHES IN THE FM INDUSTRY

SUBMITTED: December 2025
PUBLISHED: March 2026
EDITOR: Žiga Turk
DOI: 10.36680/j.itcon.2026.014

Erika Anneli Parn, Research Scientist
Division of Engineering, New York University Abu Dhabi, United Arab Emirates
eap9920@nyu.edu

Muammer Semih Sonkor, Graduate Research Assistant
Division of Engineering, New York University Abu Dhabi, United Arab Emirates
semih.sonkor@nyu.edu

Borja García de Soto, Associate Professor
Division of Engineering, New York University Abu Dhabi, United Arab Emirates
garcia.de.soto@nyu.edu

Soheila Kookalani, Research Associate
Civil Engineering Department, University of Cambridge, United Kingdom
sk2268@cam.ac.uk

SUMMARY: *Facilities Management (FM) is undergoing a rapid transformation driven by the adoption of IoT devices, building management systems, and building information models. This disruptive shift introduces significant cybersecurity threats, posing risks to safety, data privacy, and operational continuity. This paper investigates which specific configurations of organizational, technological, and human factors lead to cybersecurity breaches within FM environments. Moreover, there is a notable gap within the FM literature in terms of comprehensive understanding and strategic readiness regarding cybersecurity threats. To address this gap, this paper presents findings from an extensive survey involving 114 FM professionals who experienced cybersecurity breaches. A Fuzzy-set Qualitative Comparative Analysis (fsQCA) was utilized to identify ten distinct pathways and combinations of organizational, technological, and human factors that commonly lead to cybersecurity incidents. The analysis revealed ten distinct configurations where limited internal preparedness, financial constraints, and insufficient awareness converge to create sufficient conditions for a breach. These findings provide FM practitioners and security officers with a diagnostic taxonomy of "vulnerability profiles," allowing them to prioritize interventions based on their specific organizational constraints. This research establishes a foundation for longitudinal studies to test how these breach configurations evolve as FM systems become increasingly autonomous and integrated.*

KEYWORDS: *facilities management, cyber security, fsQCA, configurational analysis, organizational theory, digital asset management.*

REFERENCE: *Parn, E. A., Sonkor, M. S., García de Soto, B., & Kookalani, S. (2026). Pathways to cyber peril: Ten configurational routes to cybersecurity breaches in the FM industry. Journal of Information Technology in Construction (ITcon), 31, 332-352. https://doi.org/10.36680/j.itcon.2026.014*

1. INTRODUCTION

In the rapidly evolving landscape of Facilities Management (FM), the reliance on digital technologies has grown exponentially (Olimat *et al.*, 2023). Integrating smart systems, Internet of Things (IoT) devices, and complex network infrastructures elevated the operational efficiency of facilities to unprecedented levels. However, with this technological advancement comes a heightened risk of cybersecurity threats that can undermine the safety, privacy, cost-effectiveness, and functionality of these critical infrastructures (Boyes, 2015; Ghadiminia *et al.*, 2021; E. Pärn *et al.*, 2024; E. A. Pärn and García de Soto, 2020; E. Pärn and Edwards, 2019).

Cybersecurity in the FM sector is of paramount importance due to several key reasons. Firstly, FM often involves overseeing a vast array of interconnected systems (at a single site or across multiple sites) (Nota *et al.*, 2021) that control everything from heating and ventilation to security access controls and fire safety systems. A breach in cybersecurity can lead to significant disruptions, compromising the integrity of physical assets and endangering occupants and sensitive data (Coning and Mouton, 2020; Karabacak *et al.*, 2016). Secondly, facilities managers are custodians of substantial volumes of data, including personal information of employees, tenants, visitors, and customers, as well as proprietary business information. Protecting this data against unauthorized access, theft, or damage is a legal and ethical responsibility that the FM sector cannot afford to overlook (Coning and Mouton, 2020). Furthermore, the FM sector's cybersecurity preparedness is also a matter of compliance and governance. With regulations becoming more stringent around data protection and privacy (Novaes Neto *et al.*, 2021), such as the General Data Protection Regulation (GDPR) (EU, 2016) in the European Union or the California Consumer Privacy Act (CCPA) (California State Legislature, 2018) in the United States, facilities managers must ensure their cybersecurity measures meet these standards to avoid legal repercussions and maintain trust among stakeholders.

Despite the clear risks and FM's critical role in the operational integrity of built environments, the sector often faces cybersecurity preparedness and awareness challenges (Ghadiminia *et al.*, 2021). These challenges are due to a combination of factors, including the complexity of facility systems, the diverse range of technologies employed, and the varying levels of cybersecurity expertise among FM professionals. Additionally, there is often a perception among FM professionals that they do not bear the organizational responsibility for cybersecurity, or they believe that the risk can be mitigated through insurance (Hui *et al.*, 2019), further complicating the implementation of effective security measures. The sector requires a strategic approach encompassing risk assessment, continuous monitoring, incident response planning, and ongoing education on cybersecurity trends and threats.

Besides the challenges within the sector, a striking gap exists in comprehensive understanding and strategic preparedness for cybersecurity threats in the body of literature. While previous research has investigated isolated aspects of cybersecurity in facilities operations, there is a noticeable deficiency in studies that holistically examine the factors leading to cybersecurity incidents within FM. The existing literature has focused on either technical vulnerabilities or human factors contributing to cyber risks, often overlooking the complex interplay between organizational, technological, and human elements. Moreover, there is a lack of empirical research employing configurational approaches to understand how combinations of different conditions may lead to cybersecurity breaches.

This paper acknowledges that there is no singular pathway to a breach (Goh *et al.*, 2023); instead, there are as many avenues for cyber incidents as there are organizational approaches to digital integration and preparedness. Therefore, this research aims to fill the research gap by employing a nuanced Fuzzy-set Qualitative Comparative Analysis (fsQCA) methodology to identify and analyze the configurations of conditions (i.e., pathways) that most commonly lead to cybersecurity incidents in the FM sector. By moving beyond traditional variable-centric research, this paper seeks to provide a nuanced understanding of how different factors combine to create vulnerabilities or strengthen cybersecurity, reflecting the multifaceted and interconnected nature of cyber risks in the modern world. This approach allows for a more in-depth exploration of the causal complexity and provides actionable insights to facilities managers to develop comprehensive, context-specific cybersecurity strategies. In doing so, facilities managers can protect their operations and assets and contribute to the broader goal of establishing resilient and secure enterprise and urban infrastructures.

This paper is guided by a set of clearly defined objectives and research questions aimed at dissecting the intricate landscape of cybersecurity within the FM sector. The primary objectives are to comprehensively map the diverse cybersecurity attack vectors encountered by FM professionals, evaluate the extent of cybersecurity preparedness

across various FM organizations, and identify the common configurations of factors that lead to cybersecurity incidents within the sector. Accordingly, this paper seeks to answer three key research questions: (1) What are the most prevalent cybersecurity threats facing the FM sector today? (2) How do different organizational approaches to digitalization and cybersecurity preparedness influence the vulnerability of FM operations to cyber incidents? (3) What configurations of organizational, technological, and human factors most commonly lead to cybersecurity breaches in FM?

To fulfill these objectives and answer the research questions, this paper represents the most extensive survey of its kind to date, conducted with facilities managers through the International Facility Management Association (IFMA), which has generously disseminated the comprehensive questionnaire to its extensive network of professionals, thereby ensuring a broad and detailed dataset from which to draw findings. This paper contributes to the field of cybersecurity within FM by unveiling unique configurations that commonly lead to cyber incidents through a meticulous fsQCA. The findings offer novel examples of the nuanced ways that various factors converge to undermine cybersecurity in FM. They provide a foundation for developing targeted interventions and policies that address the unique challenges facing facilities managers as they safeguard their operations against cyber threats. The richness of the data, the breadth of the dimensions considered, and the use of fsQCA in this context position this paper as a new reference for researchers and practitioners aiming to fortify the cybersecurity landscape in the FM sector.

2. LITERATURE REVIEW

This paper is anchored in a constellation of theoretical frameworks that illuminate cybersecurity's multifaceted nature in the FM industry. *Complex systems theory* studies dynamic, co-evolving interactions between elements whose states change over time (Thurner *et al.*, 2018). In this paper, it provided a foundation for understanding the FM sector as an intricate web of interdependent components, where cybersecurity incidents can emerge not only from individual vulnerabilities and weaknesses but also from interactions between various system elements. By acknowledging that FM systems are complex and dynamic, this research approach focuses on configurations of factors rather than isolated variables. fsQCA is particularly suited to identifying how different conditions combine to create pathways to cyber incidents, embracing the complexity and interdependency inherent in FM systems.

Miller (1986, p. 235), a prominent organizational theorist and researcher, highlighted the importance of configurations by stating, *"The elements seem to form common gestalts such that each can best be understood in relation to the other elements in the configuration. It is the very fact that we conceive of such configurations that makes it possible for us to order our world of organizations in a rich and holistic way."* Following this line of thought, *configuration theory* further supported the methodological approach, emphasizing that multiple pathways, rather than a single deterministic cause, can lead to the same outcome, cybersecurity breaches for this paper, a concept known as equifinality in fsQCA methodology (Bertalanffy, 1968). This understanding guided the use of fsQCA to uncover the specific combinations of conditions associated with increased cyber risk, where dimensions such as "cybersecurity knowledge" and "barriers to cybersecurity" are treated as a potential part of these configurations rather than independent predictors of cyber incidents.

Cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (NIST, 2024), structured the investigation into cybersecurity preparedness within FM. These frameworks informed the selection of dimensions for fsQCA, including threat identification, protective measures, and response planning, ensuring the analysis is rooted in industry-standard practices and presents a comprehensive view of cybersecurity management. The *resource-based view (RBV)* is a management theory that explains how organizations achieve a sustainable competitive advantage by utilizing unique, valuable, and difficult-to-imitate resources (Barney, 1991; Wernerfelt, 1984). It informed the inclusion of resources and capabilities within the dimensions for fsQCA, assuming that internal resources, such as cybersecurity knowledge and asset management, contribute to cybersecurity preparedness. The fsQCA method enabled examining how these resources interact with external threats and organizational behavior to influence cybersecurity outcomes.

The *technology-organization-environment (TOE) framework*, introduced by Tornatzky et al. (1990), is a theoretical model that explains how organizations adopt technological innovations. It helped contextualize this paper by asserting that technological, organizational, and environmental factors collectively shape cybersecurity adoption and effectiveness. The TOE framework guided the selection of dimensions within fsQCA, ensuring that elements such as technological advancements, organizational policies, and regulatory environments were incorporated into

the analysis. *Institutional theory* explains how organizational behavior is shaped by evolving social environments (Roszkowska-Menkes, 2023). DiMaggio and Powell (1983) indicated that organizations are influenced by three main institutional pressures: coercive (arising from laws, regulations, and compliance requirements), normative (stemming from professional standards and industry best practices), and mimetic (mimicking successful peers). Building on this perspective, it can be inferred that institutional norms and expectations regarding cybersecurity influence organizations within the FM industry. Institutional theory underpinned the research approach in this paper by highlighting the importance of industry standards and regulations as dimensions within fsQCA, allowing exploration of how institutional pressures shape cybersecurity practices and preparedness.

Risk management theory outlines the process of estimating, evaluating, minimizing, and controlling risks by assessing their likelihood, frequency, and contributing factors (Modarres, 2016). This theoretical lens reinforced the inclusion of risk perception and management strategies as key dimensions for fsQCA. This research incorporated the systematic processes of identifying, assessing, and responding to cybersecurity risks as described by this theory, providing a structured approach to uncovering the risk management configurations that exist within the FM industry. *Fuzzy logic*, first proposed by Zadeh (1965), is a mathematical framework that extends classical logic, which operates on strict binary values (i.e., true/false), by allowing for degrees of truth. This approach enables reasoning with uncertainty and imprecision, making it particularly useful in complex systems. As the mathematical foundation of fsQCA, fuzzy logic supports this paper's methodological approach by allowing for the assessment of cybersecurity conditions as a matter of degree rather than binary presence or absence. This flexibility is particularly relevant when handling real-world data's ambiguity and partial membership characteristics, which are especially pertinent when considering the gradations of awareness, preparedness, and response capabilities within the FM industry.

By applying these theoretical frameworks, this paper employs fsQCA to dissect the intricate and often subtle interplay of factors that can precipitate cybersecurity breaches. The measured dimensions are directly informed by these theories, providing a robust, theory-driven foundation for the analysis and ensuring that the findings are deeply rooted in academic rigor and practical relevance.

2.1 Cybersecurity in facilities management

The FM industry has increasingly been relying on digital infrastructure and automation, increasing efficiency but also raising cybersecurity concerns. Several studies discussed the cybersecurity implications of this digitalization and suggested solutions for the sector. One of the primary cybersecurity risks in FM is the recently increasing integration of Building Information Modeling (BIM) into projects. Ghadiminia et al. (2021) explored these risks, emphasizing that the increasing digitalization of FM processes supported by building management systems (BMSs), BIM, and IoT devices heightens vulnerabilities to cyber threats during the post-occupancy phase. Their study revealed that FM organizations excessively rely on technology for cybersecurity management, neglecting the critical roles of people and processes. They introduced a BIM-FM cybersecurity risk matrix to illustrate the potential impacts of cyberattacks on facility operations.

Coning and Mouton (2020) examined the cybersecurity risks associated with the management of large-scale infrastructures involving several systems, such as electrical infrastructure, BMSs, heating, ventilation, and air conditioning (HVAC), and physical security systems. They highlighted the potential consequences of cyberattacks on these systems, including operational disruptions and financial losses, and proposed a mitigation framework that incorporates both technical defenses and cybersecurity training for staff. Their study emphasized the critical role of the human element in cybersecurity and suggested awareness programs for FM organizations to inform employees about potential attacks. Mantha et al. (2021) proposed a framework for cyber threat modeling that can be used by the architecture, engineering, and operations (AEC) industry during any project phase, including post-occupancy. They demonstrated the proposed framework's implementation during the commissioning phase, emphasizing that the cyber threats overlooked during this stage can significantly impact the post-occupancy phase and, thus, FM operations.

Roosmale et al. (2024) investigated the role of BIM, AI, and building automation and control systems (BACS) in modern FM, highlighting the changing scopes of FM organizations due to the increasing focus on energy efficiency, sustainability, and comfort levels in buildings. The study also identified significant cybersecurity risks associated with BACS, particularly due to their connectivity through the internet, which exposes them to attacks, such as signal corruption, data theft, and system disruptions at multiple levels. To ensure secure and resilient FM

operations, the study underscores the need for continuous cybersecurity testing and improved defense mechanisms considering human interactions. Lastly, Pavlík et al.'s study (2021) presented the increasing cybersecurity risks and threats due to digitalization in healthcare facilities, showing their impact on FM processes. They used the identified impacts to assess several security mechanisms. The study suggested that a systematic approach to identifying the impacts of cyber threats should be utilized, particularly in securing hospital information systems, focusing on both technical (e.g., hardware, software) and non-technical elements (e.g., reputation damage).

In summary, the emerging literature indicates FM systems face substantial and growing threats as facilities adopt more integrated, internet-connected technologies. Widespread weaknesses remain in organizational policies, staff practices, and technical defenses. Experts advise systematically analyzing risks, applying cybersecurity standards, training personnel, and increasing leadership focus on this issue. Addressing these areas will help improve FM's cyber resilience as a critical infrastructure sector.

2.2 Cyberattack lifecycle models and incident taxonomies

Over the years, models depicting cyberattack lifecycles shifted from linear, stage-based frameworks to multi-dimensional approaches that better reflect the complexity of modern cyber threats. One of the early and foundational examples is the Cyber Kill Chain (CKC), introduced by Lockheed Martin in 2011 (Das *et al.*, 2025). It introduced a model that involves seven stages (i.e., reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives) and has been widely adopted by various industries and government agencies (Kazimierczak *et al.*, 2024). Some of the advantages of CKC are its focus on the human element as opposed to other models that are primarily focused on technology and its comprehensiveness (Naik *et al.*, 2022). However, researchers emphasized its limitations due to its linear structure (Das *et al.*, 2025; Kazimierczak *et al.*, 2024) and developed complementary frameworks, including the Diamond Model (Caltagirone *et al.*, 2013) that captures the relational elements among the adversary, capability, infrastructure, and victim. It formalizes intrusion analysis using scientific principles to improve the effectiveness and accuracy of cyber investigations (Naik *et al.*, 2022). It also enables richer, context-aware indicators for better threat-intelligence sharing (Naik *et al.*, 2022).

Parallel to lifecycle modeling efforts, the cybersecurity community has developed standardized taxonomies and classification frameworks to enable consistent incident reporting, analysis, and information sharing across organizations and government bodies. The MITRE ATT&CK framework (MITRE, 2026) is a widely used knowledge base and taxonomy of adversary techniques, organized across the phases of the cyberattack lifecycle. It supports incident analysis by classifying attacker behaviors. On the other hand, taxonomies such as the Vocabulary for Event Recording and Incident Sharing (VERIS) framework (Verizon, 2026a) provide a common vocabulary to consistently describe cybersecurity incidents. VERIS structures incident descriptions around elements such as threat actors, actions, affected assets, and attributes, supporting aggregation and comparison of incidents across organizations and reporting programs (Menges and Pernul, 2018). At the European level, ENISA has published the Reference Incident Classification Taxonomy (ENISA, 2018), developed through collaborations involving Computer Security Incident Response Teams (CSIRTs) to support harmonized incident categorization and cross-organization information sharing.

Beyond conceptual models and taxonomies, breach research is supported by cross-sector datasets and large-scale incident compilations such as Verizon's Data Breach Investigations Report (DBIR) (Verizon, 2025), which aggregates contributed incident and breach cases. It uses the VERIS schema to enable consistent categorization of incidents. The DBIR 2025 analyzed 22,052 security incidents, including 12,195 confirmed breaches, illustrating the scale of empirical evidence available for studying breach patterns. In addition, the VERIS Community Database (VCDB) provides an open repository of publicly disclosed incidents coded in VERIS format, supporting breach research and enabling comparative analyses across incident types and sectors (Verizon, 2026b).

3. METHODOLOGY

This paper utilizes a cross-sectional, survey-based research design to collect perceptions of cybersecurity preparedness from FM professionals. A comprehensive questionnaire was developed to gather data about cybersecurity vulnerabilities, controls, and incidents across multiple dimensions. Appendix A presents the questions (annotated as Q) involved in the questionnaire under different dimensions (annotated as D) analyzed in this paper.

A plethora of organizational factors play a pivotal role in shaping the cybersecurity preparedness of the FM industry. These factors are highly intricate and subject to constant change, making them the most influential elements in cyber incidents of facilities. The phenomenon of multi-factor coupling presents a typical multi-condition configuration relationship, necessitating a method that can effectively analyze such complexity. In studying the cybersecurity preparedness of the FM industry, the small sample analysis of the qualitative comparative analysis (QCA) method proves suitable.

Specifically, fsQCA was chosen as the research method for several reasons. Firstly, this method allows for the exploration of core factors and the paths leading to cybersecurity incidents, which are influenced by multiple factors, aligning with the requirements of the study (Ragin, 2009). Secondly, fsQCA enables the exploration of the configuration relationship between multiple factors and configuration equivalence, offering more advantages than other QCA methods. Lastly, in analyzing small- to medium-sized sample cases, fsQCA presents distinct advantages over regression analysis, making it a suitable choice for studying cybersecurity preparedness in the facilities management industry (Sager and Andereggen, 2012). Figure 1 presents the process flow diagram for the methodology, with each step explained in detail in the following subsections.

Figure 1: Process flow diagram for the methodology.

3.1 Survey development

An extensive review informed the content and structure of the survey instrument, incorporating cybersecurity principles, industry frameworks (e.g., NIST CSF), and findings from past literature. The questionnaire was shared with a panel of cybersecurity experts from various FM-related industries and professional associations in January and February 2023 to validate the survey design. This expert panel, consisting of over 30 collective years of experience managing cyber risks in the FM domain, provided critical feedback on the relevance, completeness, and clarity of the survey questions. Additionally, a small pilot study was conducted by gathering input from a sample of potential respondents. This enabled further refinement of the terminology, scales, and overall survey flow before full dissemination.

3.2 Survey dissemination and data collection

To reach a large, diverse set of FM professionals, IFMA assisted with data collection by widely distributing the survey to its membership base. IFMA's membership included over 24,000 FM practitioners from 100+ countries at the time of distribution. From IFMA's 24,000 members, the survey was sent to 15,022 members who actively manage facilities, excluding consultants, students, academics, and other FM-affiliated but nonpracticing members. This provided an ideal sampling frame of informed professionals covering many organization types and industries utilizing FM services.

The finalized questionnaire was converted into an electronic format using the Qualtrics online survey platform for ease of distribution and response recording. Access to the anonymous survey was provided to 15,022 IFMA members through e-mail campaigns and online promotion over a four-month timeframe (April - July 2023). By the conclusion of data collection, the survey garnered 372 responses. The total number of valid and complete responses of FM professionals who experienced and did not experience a breach included 210 responses.

For the purposes of developing an interpretable configurational typology aligned with our research objective on the equifinality of failure, we first filtered the dataset to include only cases where a cybersecurity breach had occurred. This breach-only subset treats "breach" as a shared realised outcome to be deconstructed, rather than a dependent variable to be predicted and supports a granular exploration of how diverse configurations of organisational and technical conditions conjuncturally characterise breach contexts. Accordingly, responses where professionals stated they had not experienced any breaches or were unaware whether breaches had occurred were excluded from the typology-development stage, alongside incomplete responses. After this screening, 114

complete and valid breach responses were retained and used to construct and label the ten pathways presented in Figure 4 as an interpretable set of 'breach-context vulnerability profiles'. To ensure analytical transparency and to evaluate the breach-specificity (discriminating power) of each pathway, we additionally computed standard fsQCA sufficiency diagnostics (consistency, raw coverage, and PRI) on the full analytic sample including both breach and non-breach cases, as reported in Appendix B. While traditional QCA often seeks to explain the presence versus absence of an outcome, our research objective is specifically focused on the equifinality of failure. By constraining the pathway development stage to breach cases, we treat the 'breach' not as a binary dependent variable to be predicted, but as a shared realised outcome to be deconstructed. This allows for a granular exploration of how diverse configurations of organisational and technical weaknesses 'conjuncturally' characterise breach contexts and produce multiple, distinct vulnerability profiles within global FM settings.

3.3 Scope and boundary conditions

While this paper maps the diverse configurations leading to cybersecurity breaches, it is important to define the analytical scope regarding the dependent variable. From a technical cybersecurity standpoint, incidents can be categorized by attack vectors (e.g., phishing, ransomware) or severity levels. However, this research intentionally adopts a consolidated "breach occurrence" (Y=1) as the focal outcome.

The rationale for this boundary condition is twofold. First, this paper is grounded in the principle of equifinality, which seeks to identify the plethora of distinct organizational and technical "routes" that converge upon a singular state of system failure. Treating the breach as a shared outcome allows for a more robust deconstruction of the conjunctural weaknesses that make an organization sufficient for a realized threat, regardless of the specific technical vector used by an attacker. Second, from a configurational perspective using fsQCA, further fragmenting the outcome into sub-types would diminish the parsimony of the models and the ability to identify broad "vulnerability profiles" that are actionable for FM practitioners. Thus, the analytical depth of this paper lies in uncovering the systemic precursors to organizational peril rather than the technical taxonomies of the attacks themselves.

3.4 Fuzzy-set qualitative comparative analysis

This paper employed fsQCA as one of the primary analytical techniques. A few key factors justify its use for addressing this paper's research questions: the ability to handle complexity, accommodating diverse causal configurations (Sager and Andereggen, 2012), integration of qualitative and quantitative methods, identification of causal conditions, and supporting a holistic understanding. The publicly available software fsQCA version 4.1, developed by Ragin and Davey (2023), was used for the analysis.

The dataset in this paper often involves multiple causal conditions that can lead to an outcome of interest, which is typical in cybersecurity studies within the FM industry. fsQCA excels in managing this complexity by allowing for the examination of various combinations of conditions that may lead to the outcome (Schneider and Wagemann, 2012), accommodating the inherent complexity of cybersecurity issues. Unlike traditional linear regression methods that assume additive effects, fsQCA enables the identification of diverse causal configurations (Fiss, 2011; Ragin, 2009; Sager and Andereggen, 2012). This is particularly advantageous in this paper, as cybersecurity vulnerabilities in FM may stem from various factors, such as organizational policies, technological infrastructure, and human practices (Fiss, 2011).

Given this paper's niche focus on the FM industry, where obtaining large datasets may be challenging, fsQCA provides a suitable analytical approach. It can yield meaningful insights even with relatively small- to medium-sized samples, making it well-suited to this paper's requirements. fsQCA bridges the gap between qualitative and quantitative analysis by allowing researchers to incorporate both data types effectively. This integrative approach is invaluable in this paper for a comprehensive analysis of cybersecurity issues, which often involve a blend of qualitative assessments and quantitative measurements.

fsQCA enables the identification of necessary and/or sufficient conditions for the outcome of interest. This capability is particularly relevant to this paper, as the aim is to discern the critical factors that significantly contribute to cybersecurity resilience in FM, thereby informing targeted interventions and strategies. fsQCA provides a holistic understanding of the causal complexity inherent in cybersecurity breaches. By identifying necessary and sufficient conditions or combinations of conditions that lead to breaches, fsQCA can offer insights

into the multifaceted nature of cybersecurity vulnerabilities within FM, which may not be apparent through traditional statistical methods. By employing fsQCA in the analysis, this paper aims to provide a more granular understanding of the multifaceted dynamics underlying cybersecurity in the FM industry.

3.5 Construct dimensions in fsQCA

Through a meticulous fsQCA, respondents' perceptions were measured utilizing seven internal and external dimensions. As presented in Appendix A, each dimension (D1-7) included several questions (Q1-7) that were assessed using a 7-point Likert scale (Table 1). Each question has sub-questions referring to sub-dimensions presented with relevant abbreviations, as shown in Appendix A. For example, D2 (i.e., perception of threats) has three sub-dimensions (TFIN, TOPR, and TCYBERSEC) referring to financial, operational, and cybersecurity risks that organizations face. The dimensions utilizing each scale are presented in the top row of Table 1. The purpose and scope of each construct dimension are presented below.

D1. Knowledge: This dimension measures the level of knowledge and understanding of digital transformation and cybersecurity within the FM organization. It may include factors such as training, education, and awareness programs.

Table 1: Scales of measure for fsQCA construct dimensions.

Numerical value	Knowledge Scale (D1)	Risk Scale (D2)	Agreement Scale (D3, D6, D7)	Barrier Scale (D4)	Criticality Scale (D5)
1	No knowledge	Not at all risky	Completely disagree	No barrier at all	Not critical at all
2	Little to no knowledge	Slightly Risky	Disagree	Very minor barrier	Very minorly critical
3	Minimal knowledge	Somewhat Risky	Somewhat disagree	Minor barrier	Minorly critical
4	Basic knowledge	Moderately Risky	Neither disagree nor agree	Moderate barrier	Moderately critical
5	Adequate knowledge	Risky	Somewhat agree	Major barrier	Majorly critical
6	Very good knowledge	Very Risky	Agree	Very major barrier	Very majorly critical
7	Expert knowledge	Extremely Risky	Completely agree	Extreme barrier	Extremely critical

D2. Perception of Threats: This dimension assesses the perception of cyberattacks' potential risks and threats. It considers how well the organization recognizes and comprehends the nature and severity of cyber threats.

D3. Cybersecurity Preparedness: This dimension evaluates the organization's level of preparedness to prevent and respond to cyber breaches. It includes measures such as having cybersecurity policies and procedures, incident response plans, business continuity management, and regular audits and assessments.

D4. Perception of Barriers: This dimension explores the obstacles and challenges that hinder effective cybersecurity implementation within FM organizations. It may include factors such as budget constraints, resource limitations, organizational culture, and regulatory compliance issues.

D5. Perception of incident criticality: This dimension examines the degree of importance and criticality of FM assets regarding their vulnerability to cyber breaches. It assesses the understanding of the potential impact a breach could have on the organization's operations, reputation, and financial stability.

D6. Technology Turbulence: This dimension assesses the rate of technological change and the complexity of the technological environment within the FM organization. It considers how well the organization adapts to new technologies and incorporates cybersecurity measures in the face of rapidly evolving threats.

D7. Market Dynamism: This dimension measures the level of competitiveness and dynamism in the FM industry. It examines how these market conditions influence the organization's approach to cybersecurity, including allocating resources and prioritizing security measures.

These dimensions serve as the key variables for evaluating and comparing different configurations in fsQCA, providing insights into the unique combinations that contribute to cyber breaches in FM companies. In combination

with the questions relevant to dimensions (independent variables), a question was asked to be used as the outcome (dependent variable) in fsQCA. For this purpose, respondents were asked to report whether they experienced a cyber incident or not. Figure 2 shows the relationship between the dimensions and the outcome.

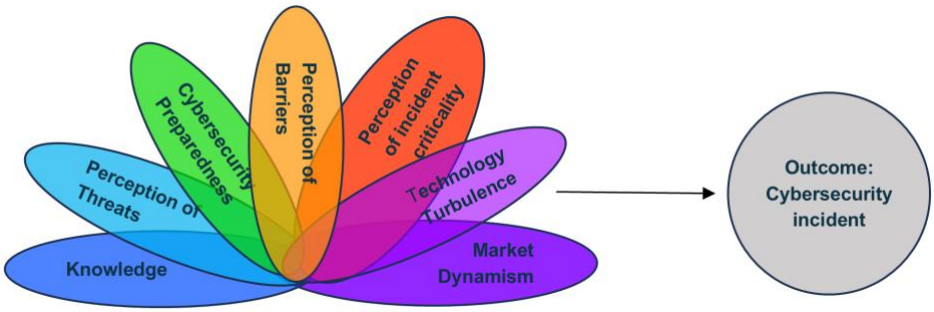

Figure 2: fsQCA dimensions and outcome.

3.6 Calibration logic

The transformation of raw survey data into fuzzy-set membership scores is a critical step for ensuring the replicability of configurational findings. The outcome variable (Breach Occurrence, Y) was calibrated as a crisp set (Y=1 for breach-reported cases; Y=0 for non-breach reported cases) for all cases included in the fsQCA. This methodological choice ensures that the identified pathways provide targeted insights into how diverse organizational and technical vulnerabilities 'conjuncturally' lead to a similar outcome, a cybersecurity breach. Table 2 details the specific calibration anchors (Full Membership, Crossover Point, and Full Non-membership) applied to each dimension. These thresholds were determined based on the qualitative descriptors of the 7-point Likert scale used in the survey instrument, ensuring that the 'gradations of awareness and preparedness' inherent in the FM industry are accurately represented.

Table 2: Calibration Logic and Fuzzy-Set Anchors.

Dimension	**Raw Scale Range**	**Full Non-Membership (0.0)**	**Crossover Point (0.5)**	**Full Membership (1.0)**	**Rationale for Calibration**
D1: Knowledge (KDIG, KCYBSEC)	1-7	1 (*No knowledge*)	4 (*Basic knowledge*)	7 (*Expert knowledge*)	Anchored by the qualitative descriptors of the scale.
D2: Perception of Threats (TOPR, TCYBERSEC, TFIN)	1-7	1 (*Not at all risky*)	4 (*Moderately risky*)	7 (*Extremely risky*)	Identifies the threshold where risk transitions from low to critical.
D3: Cybersecurity Preparedness	1-7	1 (*Completely disagree*)	4 (*Neither agree nor disagree*)	7 (*Completely agree*)	Captures the degree of organizational readiness based on agreement.
D4: Perception of Barriers	1-7	1 (*No barrier at all*)	4 (*Moderate barrier*)	7 (*Extreme barrier*)	Defines the severity of obstacles hindering implementation.
D5: Incident Criticality	1-7	1 (*Not critical at all*)	4 (*Moderately critical*)	7 (*Extremely critical*)	Maps the perceived impact of a breach on the organization.
D6/D7: Tech Turbulence & Market Dynamism	1-7	1 (*Completely disagree*)	4 (*Neither agree nor disagree*)	7 (*Completely agree*)	Measures the presence of external environmental pressures.
Outcome: Breach Occurrence (Y)	Binary	0 (No Breach Reported)	N/A (Direct Calibration)	1 (Breach Reported)	Breach occurrence is calibrated as a crisp set (Y=1 breach; Y=0 no breach). The ten pathways are labelled using breach cases, and Appendix B reports full-sample sufficiency diagnostics (consistency, coverage, PRI) to assess breach-specificity.

4. RESULTS

The analysis of survey responses provided valuable insights into the state of cybersecurity preparedness among FM professionals. This section presents an overview of the key findings.

4.1 Descriptive statistics

This section presents a descriptive overview of the collected responses ($N = 114$) and provides visualizations using box plots. In addition to the default statistical values of box plots, including the upper and lower extremes, upper (75%) and lower (25%) quartiles, and median, arithmetic mean values were also added. The median is shown with a red horizontal line, and the arithmetic mean is presented using a blue dot and the corresponding numerical value. All statistical values are between 1 and 7 due to the 7-point Likert scale used in this paper. All box plots are shown in Figure 3.

The cybersecurity awareness of FM organizations can be considered closely related to the overall *knowledge* of digital transformation (KDIG) and cybersecurity concepts (KCYBSEC). According to the results, most participants believe that their organizations have a high level of knowledge in these areas (KDIG: $M = 4.59$, standard deviation (SD) = 1.25; KCYBSEC: $M = 4.40$, $SD = 0.99$). FM professionals' *perception of threats* is a critical determinant of proactive risk management and preparedness. The data reveal that participants perceive operational risks (e.g., disruptions due to labor strikes) (TOPR: $M = 2.90$, $SD = 1.81$) as less significant than financial (TFIN: $M = 3.33$, $SD = 1.63$) and cybersecurity (TCYBERSEC: $M = 3.57$, $SD = 1.67$) risks. Moreover, the average scores for all three subdimensions, including the perception of cyber threats (TCYBERSEC), are relatively low.

FM organizations' cybersecurity preparedness reflects the extent of proactive measures implemented. The results indicate that FM organizations are better prepared in terms of having cybersecurity policies (CYBERSECPOL: M = 5.33, SD = 1.74) and trainings (PREPTRN: M = 5.35, SD = 1.91) compared to having cybersecurity policies for their facilities' BMSs (PREPBMS: M = 4.66, SD = 1.80). High SD values suggest significant variation among responses. A range of barriers (BARLOI, BARRA, BARLEG, BARCOMP, BARDTMNG, BARKNG, BARMNGT, BARMA, BARTEC) affects the adoption of cybersecurity practices in FM organizations. Among these, the level of investment on cybersecurity preparedness (BARLOI: M = 3.28, SD = 1.76), utilized legacy systems (BARLEG: M = 3.65, SD = 1.68), system compatibility (BARCOMP: M = 3.64, SD = 1.58), and the cybersecurity knowledge of employees (BARKNG: M = 3.46, SD = 1.50) appear to be particularly prominent barriers in the FM sector.

FM professionals' perception of incident criticality (CRTFINL, CRTILOS, CRTBR, CRTLOP, CRTIP, CRTSUP, CRTHL, CRTCS) reflects their assessment of the impact of cybersecurity breaches. The findings indicate that financial loss (CRTFINL: M = 4.72, SD = 1.78), confidential information exposure (CRTILOS: M = 5.27, SD = 1.69), and reputation damage (CRTBR: M = 4.80, SD = 1.86) are perceived as highly critical outcomes of cyber incidents for FM companies. On the other hand, losing partners or suppliers (CRTSUP: M = 4.07, SD = 2.06) is perceived as the least critical outcome among the eight aspects assessed. Technology turbulence captures the rate of technological change and its implications for the FM industry. The results (TECHTURB1: M = 4.84, SD = 1.54; TECHTURB2: M = 5.52, SD = 1.43; TECHTURB3: M = 4.95, SD = 1.43) suggest that FM professionals acknowledge a high level of technological disruption in the industry. Finally, the market dynamism (MARKDYN1, MARKDYN2, MARKDYN3, MARKDYN4) in FM shapes cybersecurity strategies, as rapidly changing conditions demand adaptive security measures. The findings show that FM professionals recognize significant market dynamism in the sector, with mean scores ranging from 4.20 to 5.12. Participants particularly agreed on varying customer requirements across different customer segments (MARKDYN4: M = 5.12, SD = 1.39).

These results provide a comprehensive overview of the current state of cybersecurity preparedness and the perceptions about several aspects affecting cyber breaches within the FM industry. Further analysis will delve into the configurational patterns identified through fsQCA to uncover the underlying factors contributing to cybersecurity vulnerabilities and incidents.

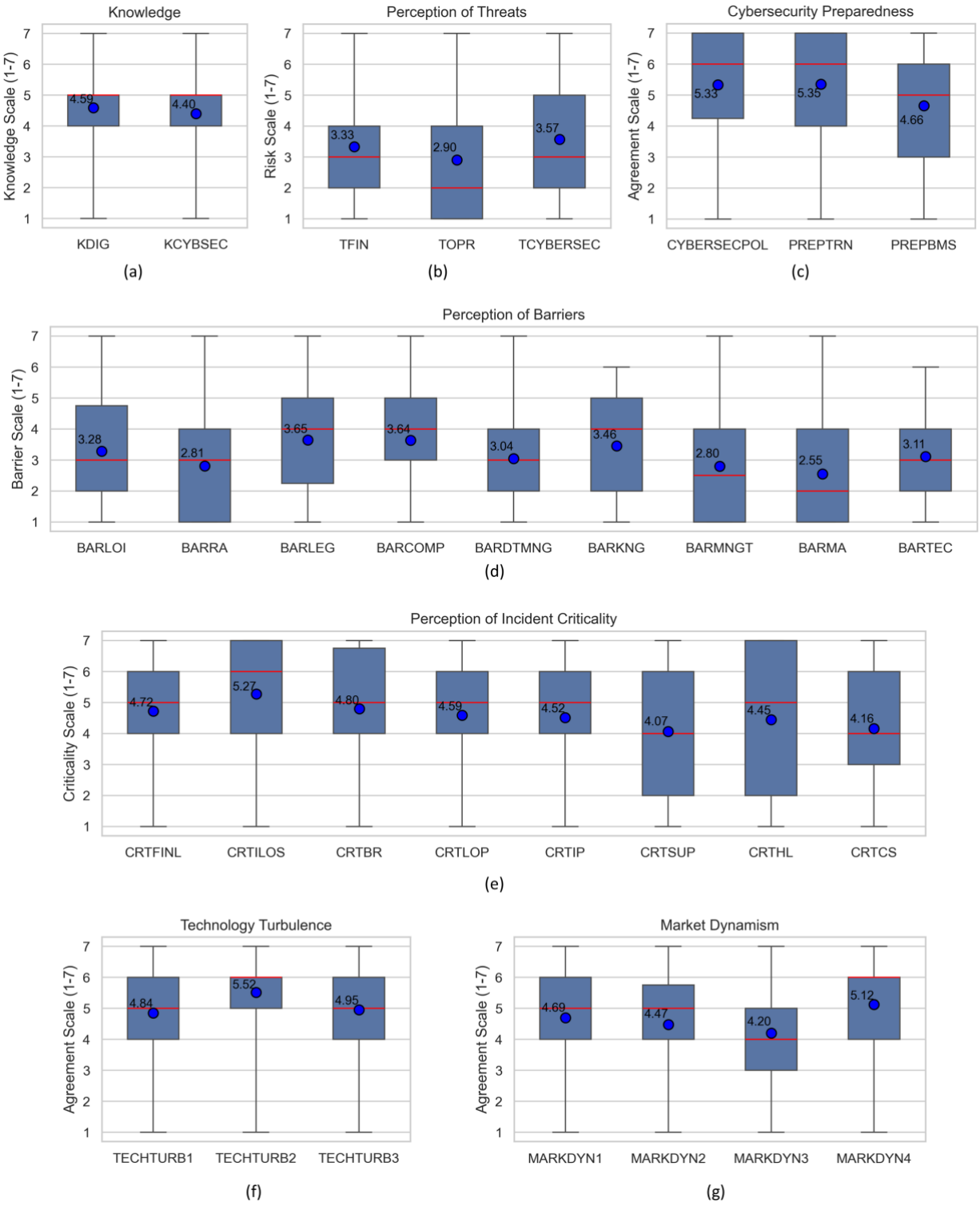

Figure 3: Box plots and average scores for the FM organizations' (a) digital transformation and cybersecurity knowledge, (b) perception of threats, (c) cybersecurity preparedness, (d) perception of barriers, (e) perception of incident criticality, (f) technology turbulence, and (g) market dynamism (N = 114).

4.2 Ten pathways to breaches

The analysis utilizing fsQCA identified ten configurations (routes), associated with cybersecurity incidents within the FM industry, as shown in Figure 4. These configurations represent different combinations of the five most significant factors (i.e., TOPR, TCYBERSEC, TFIN, TECHTURB1, MARKDYN1) that characterise equifinal vulnerability profiles in breach contexts. Appendix B reports full configurational sufficiency diagnostics (consistency, raw coverage, and PRI) for each route, enabling assessment of both empirical relevance (coverage) and breach-specificity (discriminating power). Overall, internal factors, particularly higher perceived operational (TOPR) and cybersecurity (TCYBERSEC) threats, tend to feature more prominently in the routes with stronger breach-specificity (higher PRI), whereas routes dominated by external pressures (TECHTURB1 and MARKDYN1) may exhibit higher prevalence (coverage) but weaker discrimination between breach and non-breach contexts (lower/near-zero PRI) when internal preparedness is limited. Each route is explained below.

Following the calibration anchors reported in Table 2, we provide full configurational sufficiency metrics (consistency, raw coverage, PRI) for each of the ten labelled pathways in Appendix B, computed on the full analytic sample (breach and non-breach cases) to avoid trivial consistency in breach-only subsets.

Appendix B shows that the ten theorised configurations vary markedly in both empirical relevance (raw coverage) and breach-specificity (PRI). The most prevalent pathway is Configuration 4 (External Pressure Cooker), which achieves the highest raw coverage (0.348) and high frequency, indicating it captures a large share of breach membership in the sample; however, its consistency is ~0.50 and PRI is slightly negative (−0.006), signalling that this pattern is almost equally compatible with non-breach cases and therefore has limited discriminating power. A similar issue is observed for Configuration 5 (Financial Fortress) (consistency ~0.50; PRI −0.006), suggesting it also does not uniquely characterise breached organisations. In contrast, several less prevalent pathways show stronger breach specificity: Configuration 8 (Well-Rounded Defender) and Configuration 6 (Operational Leader) exhibit the highest discrimination (PRI 0.378 and 0.360, respectively) and the highest consistencies (0.616 and 0.610), albeit with lower coverage (0.126 and 0.171), indicating they represent more selective but more breach-indicative risk signatures. Configuration 10 (Comprehensive Defender) provides a balanced profile (consistency 0.587, coverage 0.182, PRI 0.295), while Configurations 1–3 and 7–9 show moderate consistencies (≈0.52–0.56) and generally low PRI (≈0.09–0.22), implying that although these patterns are present among breach cases, they are less uniquely associated with breaches relative to non-breach cases.

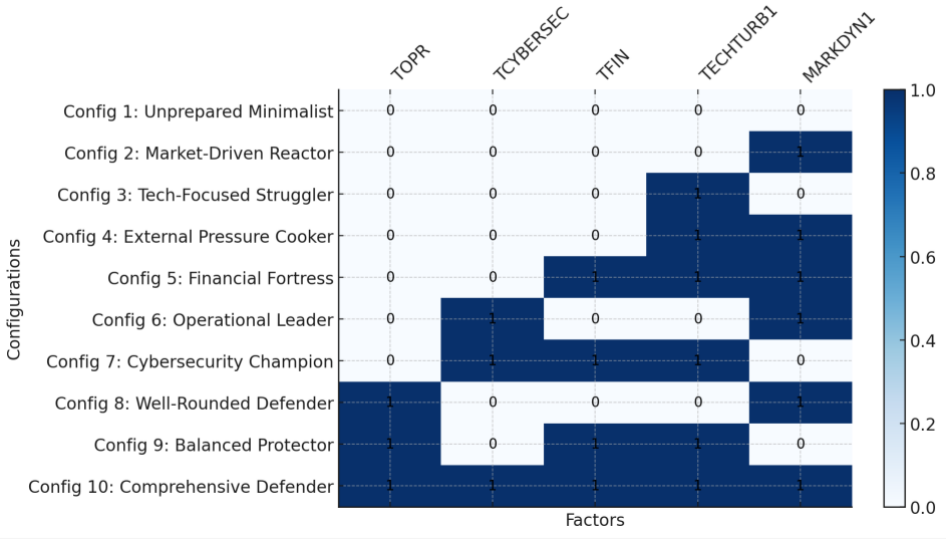

Figure 4: Key configurations from fsQCA analysis.

Configuration 1: Unprepared Minimalist – None of the factors are present. This is the most vulnerable configuration, representing an organization lacking both internal and external readiness.

Configuration 2: Market-Driven Reactor – Internal factors are absent while MARKDYN1 is present, indicating an organization reacting to external market pressures without internal preparedness.

Configuration 3: Tech-Focused Struggler – TECHTURB1 is present while internal factors are absent, indicating an organization influenced by external technological instability without internal support.

Configuration 4: External Pressure Cooker – Both external factors (i.e., TECHTURB1 and MARKDYN1) are present, while internal factors are absent, representing an organization under external pressure with low internal preparedness.

Configuration 5: Financial Fortress – TFIN, TECHTURB1, and MARKDYN1 are present, while internal factors are absent. Financial readiness (TFIN) being present indicates an organization with strong financial backing but facing external pressures from technology and markets.

Configuration 6: Operational Leader – TCYBERSEC and MARKDYN1 are present while external factors are absent, signaling a focus on internal operations but without external preparedness.

Configuration 7: Cybersecurity Champion – TCYBERSEC, TFIN, and TECHTURB1 are present, while external factors are absent. Cybersecurity preparedness (TCYBERSEC) and finances (TFIN) being strong highlights an organization focused on internal cybersecurity defense without as much attention to external pressures.

Configuration 8: Well-Rounded Defender – TOPR and MARKETDYN1 are present, representing a well-prepared organization from perceptions point of view, though external factors are absent.

Configuration 9: Balanced Protector – TOPR, TFIN, and TECHTURB1 are present, showing a balance between internal operations, financial readiness, and responsiveness to the technological turbulence of the market.

Configuration 10: Comprehensive Defender – All internal and external factors are present, signaling an organization that is both internally strong and responsive to external pressures.

These configurations provide a roadmap for defending against the industry's most critical threat categories. For instance, configurations involving high 'Technology Turbulence' (D6) combined with low 'Cybersecurity Knowledge' (D1) suggest that rapid digital adoption without corresponding training creates 'blind spots' where ransomware can be introduced via phishing or unpatched software. Furthermore, the data showed that FM organizations are significantly less prepared regarding BMS-specific policies (M=4.66) compared to general IT policies (M=5.33). This gap is particularly dangerous for configurations where 'Incident Criticality' (D5) is underestimated, as attackers can weaponize building automation systems (BMS compromise) to cause physical operational disruptions. Finally, configurations characterized by a lack of formal 'Cybersecurity Preparedness' (D3) and low 'Perception of Threats' (D2) indicate environments where insider misuse, whether intentional or accidental, is more likely to occur due to the absence of clear governance and monitoring 'guardrails'. However, the routes are not all equally prevalent: Appendix B indicates uneven raw coverage across configurations, suggesting that a smaller subset of pathways accounts for a disproportionate share of breach cases.

Overall, identifying these ten routes provides valuable insights into the complex interplay of factors that contribute to cybersecurity incidents within the FM industry. Further examination of each configuration will shed light on specific vulnerabilities and risk factors, informing targeted interventions to enhance cybersecurity preparedness and resilience in FM organizations.

4.3 High-risk configurations

Certain configurations, especially those that lack strong internal factors, are classified as high-risk. These include configurations where organizations rely heavily on external factors but lack internal preparedness, particularly in operational and cybersecurity areas. These configurations are explained and compared in Figure 5 and Table 3.

Configurations lacking strong internal factors, such as TOPR and TCYBERSEC, exhibit heightened vulnerability to cybersecurity risks. Moreover, reliance on external factors, as demonstrated by configurations such as the Market-Driven Reactor and Tech-Focused Struggler, underscores the risks associated with insufficient internal controls.

In addition to the high-risk configurations, configuration 5 (i.e., Financial Fortress) was identified as a medium-risk configuration. In this configuration, financial readiness is present, which provides a degree of protection; however, it remains vulnerable due to external pressures from technology and market dynamics. Despite financial stability, the absence of operational or cybersecurity preparedness increases risk under external pressures.

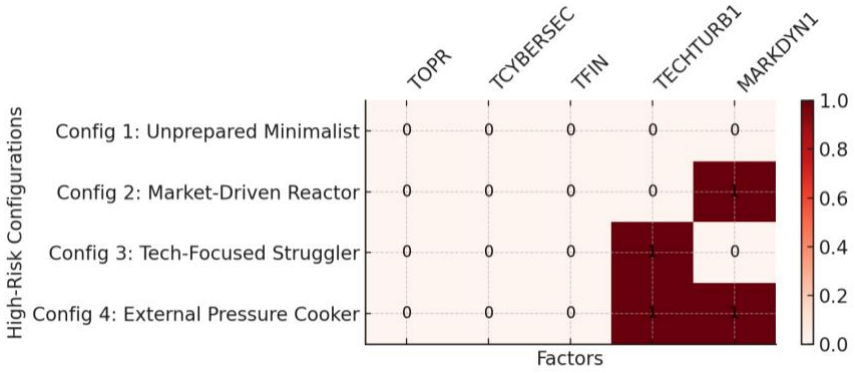

Figure 5: Comparison of high-risk configurations.

Table 3: Summary of high-risk configurations.

Configuration	Risk	Reason
Configuration 1: Unprepared Minimalist	This is the most vulnerable configuration, with all factors absent. The organization is unprepared both internally and externally, leading to a high risk of cybersecurity breaches.	No internal (TOPR, TCYBERSEC, TFIN) or external (TECHTURB1, MARKDYN1) factors are present.
Configuration 2: Market-Driven Reactor	Although market dynamics (MARKDYN1) is present, all internal preparedness factors are absent. This organization relies heavily on external market pressures without the necessary internal defenses.	The absence of internal factors like cybersecurity preparedness and operational readiness increases the risk of a breach despite reacting to external market conditions.
Configuration 3: Tech-Focused Struggler	Technology Turbulence (TECHTURB1) is present, indicating that the organization is dealing with external technological instability without strong internal preparedness. This leaves the organization at high risk.	Lack of internal cybersecurity readiness and operational systems in a tech-unstable environment increases risk.
Configuration 4: External Pressure Cooker	Both external factors (technology and market dynamics) are present, indicating external pressure. However, the lack of internal preparedness makes the organization vulnerable to attacks.	The absence of internal factors in a volatile external environment creates a high-risk scenario.

4.4 Impact of perceived barriers

The presence of perceived barriers (legal, organizational, or knowledge-based) was found to significantly impact the likelihood of a cybersecurity breach. Organizations that face these barriers, particularly in combination with external pressures, are more likely to experience breaches if they do not have strong internal systems in place. The analysis revealed that knowledge-based and organizational barriers had the strongest impact on cybersecurity readiness. These barriers represent challenges in understanding cybersecurity threats or effectively managing internal operations to protect against them. Legal barriers, while still important, were found to have a lesser impact compared to knowledge and organizational barriers.

The analysis found that organizations facing significant knowledge-based barriers are often unprepared to manage cybersecurity risks. Organizational barriers, such as internal coordination and resource allocation, also play a

crucial role in determining readiness. The presence of these barriers, when combined with external pressures like market dynamics, greatly increases the likelihood of a breach.

4.5 Perceptions of asset criticality

The following factors related to criticality were analyzed: CRTFINL (financial criticality), CRTILOS (information loss criticality), CRTBR (brand reputation criticality), CRTLOP (operational criticality), CRTIP (IT infrastructure criticality), CRTSUP (supply chain criticality), CRTHL (health/life safety criticality), CRTCS (customer service criticality). The following are the observations from this analysis:

Financial and Operational Criticality: In the configuration where TOPR, TFIN, and TCYBERSEC are present, financial criticality (CRTFINL) and operational criticality (CRTLOP) were often absent, suggesting that even without the perception of these as critical, organizations with strong internal readiness still maintained strong outcomes.

IT Infrastructure Criticality: CRTIP (IT infrastructure criticality) was absent in many configurations. This suggests that organizations may not prioritize IT infrastructure as critical as they should, and this might expose them to vulnerabilities.

Brand Reputation and Customer Service Criticality: CRTBR (brand reputation) and CRTCS (customer service criticality) did not frequently appear in the key configurations, indicating that these factors are less emphasized in cybersecurity planning but could become critical if left under-protected.

Health and Supply Chain Criticality: These factors were generally absent from the configurations, suggesting that organizations may not perceive these as top priorities, but they represent potential areas of risk, especially for industries dealing with physical infrastructure or healthcare.

According to the fsQCA findings, the absence of asset criticality perceptions (e.g., CRTFINL, CRTLOP, CRTIP) generally correlates with higher vulnerability in many configurations. In cases where critical assets (e.g., IT infrastructure, financial systems) are not perceived as critical, organizations may underprioritize their cybersecurity defenses, making them more susceptible to breaches. Conversely, the presence of asset criticality perceptions can lead to greater prioritization of cybersecurity measures, reducing the likelihood of a breach. When organizations recognize the importance of critical assets, they are more likely to implement stronger protections around those assets, improving overall security outcomes.

The findings also showed that IT infrastructure (CRTIP) and operational criticality (CRTLOP) are key factors that could have a stronger influence on breach outcomes if prioritized correctly. Moreover, financial criticality (CRTFINL) is not always a determining factor in strong cybersecurity outcomes, especially if internal preparedness (TOPR, TCYBERSEC) is already in place.

4.6 Financial and operational readiness

Organizations with strong asset criticality perceptions and financial and operational readiness factors (TFIN, TOPR) are more likely to allocate sufficient resources to cybersecurity measures. In configurations where asset criticality is present, it was often seen that other factors like financial readiness (TFIN) are also present, suggesting that organizations are more prepared to invest in necessary cybersecurity measures where perceptions of asset criticality are present.

Asset criticality alone may not be sufficient to drive cybersecurity investment on its own, but it plays an important role in shaping decisions. Organizations often consider a broader context that includes internal preparedness, external pressures, and perceived risks when allocating resources to cybersecurity measures. The following are several factors that influence how asset criticality impacts investment decisions:

Perception of Risk: If an organization perceives certain assets (e.g., financial data, IT infrastructure, customer service systems) as highly critical, it is more likely to invest in protecting those assets. The perception of criticality creates a sense of urgency to ensure the safety and availability of those assets. However, this alone might not trigger investment. It typically needs to be combined with an awareness of specific cybersecurity threats to drive significant resource allocation.

Internal Preparedness: If an organization perceives its critical assets (e.g., IT systems) as highly important but also feels prepared (e.g., having strong operational readiness, utilizing cybersecurity frameworks), it may not see the need for additional investment. On the other hand, organizations with weak internal readiness but high criticality perception might prioritize investment more urgently to fill those gaps.

External Pressures: Market dynamics or technological turbulence can amplify the influence of asset criticality on investment decisions. For example, if an organization is in a rapidly changing technology landscape, it might see the criticality of IT systems as a reason to invest more heavily in cybersecurity. Similarly, industries facing high levels of regulatory scrutiny (e.g., healthcare, finance) might see critical assets driving cybersecurity investments as part of compliance measures.

Cybersecurity Breaches: Past incidents or near-misses can act as catalysts. If a critical asset (such as sensitive financial data or IT infrastructure) has been threatened or breached, this experience may drive significant investment to prevent future incidents. The experience of a breach tends to elevate the perceived criticality of certain assets and makes the need for investment more evident.

While asset criticality perception is a key factor in determining where organizations allocate resources, it often needs to be paired with other contextual factors, such as internal readiness, external pressures, and past experiences of breaches, to drive substantial investment in cybersecurity. On its own, the perception of criticality might raise awareness but not necessarily trigger investment unless the organization sees direct risks to those assets.

4.7 Comparative analysis

Comparing the results with existing literature or expected outcomes helps validate the findings and provides context for understanding the implications of this research within the broader body of knowledge. The following is how the results align with existing literature or expected outcomes:

Consistency with Previous Research: The findings are consistent with previous research highlighting the importance of factors such as organizational cybersecurity culture, technical vulnerabilities, and employee training in contributing to cybersecurity incidents (Coning and Mouton, 2020; Ghadiminia *et al.*, 2021). This consistency strengthens the validity of this paper's results and underscores the significance of addressing these factors in FM cybersecurity strategies.

Identification of Novel Pathways: While some of the findings may align with existing literature, this paper also identifies novel pathways or configurations leading to cybersecurity incidents within the FM industry. For example, the identification of Route 10, which emphasizes the role of comprehensive preparedness, may still lead to a breach for FM professionals, which may provide new insights not previously explored in the literature. This highlights the contribution of our research in expanding the understanding of cybersecurity risks in FM.

Validation of Theoretical Frameworks: The results may also validate theoretical frameworks or models proposed in previous literature. For instance, identifying certain dimensions or factors in the configurations may align with established cybersecurity frameworks (e.g., NIST CSF), lending support to their applicability in the FM context. This validation strengthens the theoretical underpinnings of this paper and provides a basis for future research and practical applications.

Addressing Gaps in Knowledge: This research may address gaps in the existing literature by providing empirical evidence on specific pathways or configurations leading to cybersecurity incidents in FM. By filling these gaps, this paper contributes to a more comprehensive understanding of cybersecurity risks and resilience in the FM industry (Coning and Mouton, 2020; Ghadiminia *et al.*, 2021; Roosmale *et al.*, 2024).

Implications for Practice: Finally, comparing the results with existing literature or expected outcomes allows drawing practical implications for FM practitioners and policymakers. By identifying key dimensions or factors associated with cybersecurity incidents, this paper's findings can inform the development of targeted interventions and strategies to enhance cybersecurity preparedness and mitigate risks in FM organizations (Pavlík *et al.*, 2021).

Surprising Finding: A particularly noteworthy finding is the identification of a 'Comprehensive Defender' configuration (Route 10). In this pathway, despite high levels of Cybersecurity Knowledge (D1), Preparedness (D3), and Internal Policy (D4), breaches still occurred. This contradicts the linear assumption that increasing 'maturity' in every dimension leads to a zero-risk state. Instead, it supports the Principle of Equifinality: in complex

FM environments, no single defensive posture is a silver bullet, and threats can still penetrate through the 'conjunctural' intersection of external turbulence and internal complexity. The occurrence of breaches within 'Comprehensive Defender' profiles must be interpreted with caution regarding incident detection bias. In the context of cybersecurity maturity models, organizations with higher maturity typically possess more robust logging, SIEM (Security Information and Event Management) systems, and specialized personnel. Consequently, these organizations are more likely to identify and report a breach (Outcome Y) than those with lower maturity who may remain in a state of 'silent compromise.' Thus, our findings suggest that as FM organizations mature, the 'Outcome Variable' (Breach) may reflect an increased visibility of threats rather than a failure of defenses alone. This highlights a critical paradox for FM managers: higher investment in cybersecurity infrastructure leads to a higher frequency of detected (and therefore actionable) incidents.

Overall, comparing the results with existing literature or expected outcomes helps situate the findings within the broader scholarly discourse, validate the research approach, and identify avenues for future investigation and practical implementation.

5. LIMITATIONS AND FUTURE RESEARCH

While this paper sheds light on a significant topic, certain limitations must be acknowledged. One potential limitation is the sampling bias inherent in the survey approach. While efforts were made to reach a diverse range of FM professionals through IFMA, the sample's composition may still be skewed toward certain demographics or organizational types. This could affect the generalizability of the findings to the broader population of FM practitioners. Secondly, this paper relies on self-reported data provided by respondents, which may be subject to biases such as social desirability or recall bias. Participants may overestimate or underestimate their organization's cybersecurity preparedness, leading to inaccuracies in the data. Additionally, respondents may be reluctant to report cybersecurity incidents due to concerns about confidentiality or reputational damage.

Another limitation is the limited scope of variables used in this paper. The survey instrument used in this paper may not capture the full spectrum of factors influencing cybersecurity incidents in FM organizations. Certain variables or dimensions relevant to cybersecurity preparedness and vulnerabilities may not have been included in the survey, limiting the depth of the analysis. Because high-maturity organisations may detect/report incidents more reliably, some configurations may partly reflect detection visibility rather than purely defensive failure. PRI values in Appendix B help flag such cases by indicating weaker discrimination between breach and non-breach. Additionally, this paper employs a cross-sectional research design, which provides a snapshot of cybersecurity preparedness at a specific point in time. This design does not allow for examining changes or trends in cybersecurity incidents over time, limiting the ability to draw causal conclusions or assess the long-term effectiveness of cybersecurity interventions.

Despite efforts to maximize response rates, this paper may have experienced challenges in engaging participants, leading to a lower-than-desired response rate. Additionally, non-response bias, where certain groups of respondents are more likely to participate than others, could impact the representativeness of our sample and introduce systematic errors into our analysis. Lastly, while fsQCA is a valuable analytical tool for exploring complex causal relationships, it also has limitations. For example, fsQCA relies on subjective judgments in coding and calibrating variables, which may introduce researcher bias.

5.1 Suggestions for future research

Several aspects that can be considered in future research are as follows:

- Conducting longitudinal studies to track changes in cybersecurity preparedness and incidents over time would provide valuable insights into trends and patterns within the FM industry. By examining how cybersecurity practices evolve and adapt in response to emerging threats and technological advancements, researchers can better assess the effectiveness of interventions and strategies over the long term.
- Complementing the quantitative survey approach utilized in this paper with qualitative research methods, such as interviews or focus groups, can offer deeper insights into the underlying factors influencing cybersecurity incidents in FM organizations. Qualitative research allows for a more nuanced exploration of organizational cultures, decision-making processes, and contextual factors that may shape cybersecurity practices.

- Conducting comparative analyses across different industries or geographic regions can help identify variations in cybersecurity practices and vulnerabilities within the FM sector. By comparing FM organizations operating in diverse contexts, researchers can identify best practices, lessons learned, and areas for improvement that may be transferable across settings.
- Given the interconnected nature of modern supply chains and their susceptibility to cybersecurity threats, further investigation into supply chain risk management practices within the FM industry is warranted. Examining the relationships between FM organizations and their suppliers, subcontractors, and service providers can shed light on potential vulnerabilities and strategies for mitigating supply chain risks.
- Exploring the role of human factors, such as employee awareness, training, and behavior, in shaping cybersecurity outcomes is essential. Investigating the effectiveness of cybersecurity training programs, employee compliance with security protocols, and the impact of organizational culture on cybersecurity culture can provide insights into strategies for enhancing human resilience to cyber threats within FM organizations.
- With the increasing adoption of emerging technologies, such as IoT devices, artificial intelligence (AI), and cloud computing, there is a need to examine their implications for cybersecurity in FM. Additionally, the connection of individual buildings to micro-grids, smart neighborhoods, and, ultimately, smart cities will lead to new challenges and vulnerabilities. As these interconnected systems grow more complex, they introduce potential points of failure and new vectors for cyber-attacks, necessitating robust and adaptive security measures to protect sensitive data and ensure the reliable operation of critical infrastructure. Research focusing on the security challenges and vulnerabilities associated with these technologies, as well as strategies for managing risks effectively, can help FM practitioners navigate the complexities of digital transformation securely.
- It is crucial to investigate the impact of regulatory frameworks and compliance requirements on cybersecurity practices in FM. Assessing the extent to which FM organizations adhere to industry standards, regulations, and guidelines, such as those set forth by regulatory bodies like NIST or ISO, can inform efforts to strengthen regulatory compliance and enhance cybersecurity governance.

6. CONCLUSION

The comprehensive data collection, conducted over two years with IFMA members, provided invaluable insights into cybersecurity within the realm of FM. Through a meticulous survey design and data collection process, this paper explored the perceptions of cyber awareness and preparedness among professionals, examining the correlation between these perceptions and the incidence of cyber-related incidents. Using a 7-point Likert scale to evaluate 114 statements across seven dimensions has yielded detailed and nuanced understandings of the existing cybersecurity configurations among FM professionals.

The findings revealed ten configurations which we have named among the participants: 1) Unprepared Minimalist, 2) Market-Driven Reactor, 3) Tech-Focused Struggler, 4) External Pressure Cooker, 5) Financial Fortress, 6) Operational Leader, 7) Cybersecurity Champion, 8) Well-Rounded Defender, 9) Balanced Protector, and 10) Comprehensive Defender. Each of these configurations encapsulates a unique blend of awareness, preparedness, and financial prioritization that impacts the cybersecurity posture of FM operations. Yet, PRI results (Appendix B) indicate that not all routes discriminate equally well between breach and non-breach contexts; therefore, the ten-route typology should be read as a map of equifinal vulnerability profiles, with stronger practical prioritisation given to pathways that combine meaningful raw coverage with stronger breach-specificity, most notably Configuration 10 (Comprehensive Defender) (coverage 0.182, PRI 0.295) and Configuration 6 (Operational Leader) (coverage 0.171, PRI 0.360), alongside the more selective but highly discriminating Configuration 8 (Well-Rounded Defender) (coverage 0.126, PRI 0.378).

The implications of these findings are twofold. Firstly, they underscore the cybersecurity challenges' complexity and multifaceted nature within the FM sector. It is evident that while some professionals are cognizant of the cyber risks and prepared to tackle them, financial constraints and a lack of comprehensive understanding regarding intellectual property (IP) protection often hinder effective cyber defense mechanisms. Secondly, the discovery of configurations, such as Market-Driven Reactor, Tech-Focused Struggler, and External Pressure Cooker, highlights the critical need for enhanced awareness programs and internal preparedness that address cyber threats and the broader implications of cyber incidents on FM.

In conclusion, this paper illuminates the imperative for a holistic approach to cybersecurity in FM. As facilities become increasingly integrated with digital technologies, the potential for cyber threats looms, making it essential for professionals in this sector to understand the risks and possess the knowledge and resources necessary to mitigate them. The intricate relationship between cyber awareness, preparedness, and financial prioritization revealed through this research points towards the need for targeted strategies that address these interdependencies. By fostering a culture of cyber-savviness and ensuring that policies are robust and practically implemented, FM professionals can better safeguard their operations against the ever-evolving landscape of cyber threats. This paper contributes to the understanding of cybersecurity within FM and underscores the importance of continuous improvement and adaptation in cyber defense strategies to protect against potential vulnerabilities.

ACKNOWLEDGMENTS

We would like to acknowledge the industry advice, support, and feedback from Jeffrey Saunders, Chief Technology Officer at the Danish National Defense Technology Centre, and Shaun Reardon, Principal Cybersecurity Consultant at DNV. This research was partially supported by different centers at New York University Abu Dhabi. In particular, the Center for Sand Hazards and Opportunities for Resilience, Energy, and Sustainability (SHORES), funded by Tamkeen under the NYUAD Research Institute Award CG013 and the Center for Cyber Security at New York University Abu Dhabi (CCS-AD), funded by Tamkeen under the NYUAD Research Institute Award G1104.

REFERENCES

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage, Journal of Management 17(1): 99–120. https://doi.org/10.1177/014920639101700108

Bertalanffy, L. von. (1968). General System Theory: Foundations, Development, Applications, G. Braziller: 978-0-8076-0453-3.

Boyes, H. (2015). Security, Privacy, and the Built Environment, IT Professional 17: 25–31. https://doi.org/10.1109/MITP.2015.49

California State Legislature. (2018). California Consumer Privacy Act (CCPA) of 2018, California State Legislature. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Caltagirone, S., Pendergast, A. and Betz, C. (2013). The Diamond Model of Intrusion Analysis. https://apps.dtic.mil/sti/html/tr/ADA586960/

Coning, A. D. and Mouton, F. (2020). Bulk infrastructure management for facilities management, Presented at the 2020 Resilience Week, RWS 2020, pp. 181–187. https://doi.org/10.1109/RWS50334.2020.9241262

Das, T., Rath, S. and Sengupta, S. (2025). GCAP: Cyber Attack Progression Framework for Smart Grid Infrastructures, IEEE Internet of Things Journal 12(3): 2906–2917. https://doi.org/10.1109/JIOT.2024.3474637

DiMaggio, P. J. and Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields, American sociological review 48(2): 147–160. http://www.jstor.org/stable/2095101?origin=JSTOR-pdf

ENISA. (2018). Reference Incident Classification Taxonomy | ENISA. https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

EU. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (No. Regulation (EU) 2016/679). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Fiss, P. C. (2011). Building Better Causal Theories: A Fuzzy Set Approach to Typologies in Organization Research, Academy of Management Journal 54(2): 393–420. https://doi.org/10.5465/amj.2011.60263120

Ghadiminia, N., Mayouf, M., Cox, S. and Krasniewicz, J. (2021). BIM-enabled facilities management (FM): a scrutiny of risks resulting from cyber attacks, Journal of Facilities Management. https://doi.org/10.1108/JFM-01-2021-0001

Goh, J. R., Wang, S. S., Harel, Y. and Toh, G. (2023). Predictive Taxonomy Analytics (LASSO): Predicting Outcome Types of Cyber Breach, J. Cybersecur. 9. https://doi.org/10.1093/cybsec/tyad015

Hui, K., Hui, W. and Yue, W. (2019). Cyber Insurance and Risk Management: A Normative Analysis, Information Systems & Economics eJournal. https://doi.org/10.2139/ssrn.3486658

Karabacak, B., Yildirim, S. O. and Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness, International Journal of Critical Infrastructure Protection 15: 47–59. https://doi.org/10.1016/j.ijcip.2016.10.001

Kazimierczak, M., Habib, N., Chan, J. H. and Thanapattheerakul, T. (2024). Impact of AI on the Cyber Kill Chain: A Systematic Review, Heliyon 10(24): e40699. https://doi.org/10.1016/j.heliyon.2024.e40699

Mantha, B. R. K., García de Soto, B. and Karri, R. (2021). Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment, Sustainable Cities and Society 66: 102682. https://doi.org/10.1016/j.scs.2020.102682

Menges, F. and Pernul, G. (2018). A comparative analysis of incident reporting formats, Computers & Security 73: 87–101. https://doi.org/10.1016/j.cose.2017.10.009

Miller, D. (1986). Configurations of Strategy and Structure: Towards a Synthesis, Strategic Management Journal 7(3): 233–249. https://www.jstor.org/stable/2486075

MITRE. (2026). MITRE ATT&CK, MITRE ATT&CK. https://attack.mitre.org/

Modarres, M. (2016). Risk Analysis in Engineering: Techniques, Tools, and Trends, CRC Press: 978-1-4200-0349-9.

Naik, N., Jenkins, P., Grace, P. and Song, J. (2022). Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model, In 2022 IEEE International Symposium on Systems Engineering (ISSE), Presented at the 2022 IEEE International Symposium on Systems Engineering (ISSE), pp. 1–7. https://doi.org/10.1109/ISSE54508.2022.10005490

NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0, NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Nota, G., Peluso, D. and Lazo, A. (2021). The contribution of Industry 4.0 technologies to facility management, International Journal of Engineering Business Management 13. https://doi.org/10.1177/18479790211024131

Novaes Neto, N., Madnick, S., Paula, A. and Borges, N. (2021). Developing a Global Data Breach Database and the Challenges Encountered, Journal of Data and Information Quality 13: 1–33. https://doi.org/10.1145/3439873

Olimat, H., Liu, H. and Abudayyeh, O. (2023). Enabling Technologies and Recent Advancements of Smart Facility Management, Buildings. https://doi.org/10.3390/buildings13061488

Pärn, E. A. and García de Soto, B. (2020). Cyber threats and actors confronting the Construction 4.0, In A. Sawhney, M. Riley, & J. Irizarry (Eds), Construction 4.0: An Innovation Platform for the Built Environment, London, UK: Routledge: 978-0-367-02730-8, pp. 441–459. https://doi.org/10.1201/9780429398100-22

Pärn, E. and Edwards, D. (2019). Cyber threats confronting the digital built environment: Common data environment vulnerabilities and block chain deterrence, Engineering Construction & Architectural Management 26(2): 245–266. https://doi.org/10.1108/ECAM-03-2018-0101

Pärn, E., Ghadiminia, N., García de Soto, B. and Oti-Sarpong, K. (2024). A perfect storm: Digital twins, cybersecurity, and general contracting firms, Developments in the Built Environment 18: 100466. https://doi.org/10.1016/j.dibe.2024.100466

Pavlík, L., Chytilová, E. and Zimmermannová, J. (2021). Security aspects of healthcare organization from the perspective of digitization of facility management, WSEAS Transactions on Business and Economics 18: 360–366. https://doi.org/10.37394/23207.2021.18.36

Ragin, C. C. (2009). Redesigning social inquiry: Fuzzy sets and beyond, University of Chicago Press: 978-0-226-70275-9.

Ragin, C. C. and Davey, S. (2023). Fuzzy-Set/Qualitative Comparative Analysis 4.1. https://sites.socsci.uci.edu/~cragin/fsQCA/software.shtml

Roosmale, S. van, Hellinckx, P., Meysman, J., Verbeke, S. and Audenaert, A. (2024). Building automation and control systems for office buildings: Technical insights for effective facility management - A literature review, Journal of Building Engineering 97: 110943. https://doi.org/10.1016/j.jobe.2024.110943

Roszkowska-Menkes, M. (2023). Institutional Theory, In S. O. Idowu, R. Schmidpeter, N. Capaldi, L. Zu, M. Del Baldo, & R. Abreu (Eds), Encyclopedia of Sustainable Management, Cham: Springer International Publishing: 978-3-031-25984-5, pp. 1983–1990. https://doi.org/10.1007/978-3-031-25984-5_389

Sager, F. and Andereggen, C. (2012). Dealing With Complex Causality in Realist Synthesis: The Promise of Qualitative Comparative Analysis, American Journal of Evaluation 33(1): 60–78. https://doi.org/10.1177/1098214011411574

Schneider, C. Q. and Wagemann, C. (2012). Set-Theoretic Methods for the Social Sciences: A Guide to Qualitative Comparative Analysis, Cambridge University Press: 978-1-107-01352-0.

Thurner, S., Klimek, P. and Hanel, R. (2018). Introduction to the Theory of Complex Systems, Oxford University Press: 978-0-19-882193-9. https://doi.org/10.1093/oso/9780198821939.001.0001

Tornatzky, L. G., Fleischer, M. and Chakrabarti, A. K. (1990). The Processes of Technological Innovation, Lexington Books: 978-0-669-20348-6.

Verizon. (2025). 2025 Data Breach Investigations Report | Verizon, 2025 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/

Verizon. (2026a). The VERIS Framework, The VERIS Framework. https://verisframework.org/index.html

Verizon. (2026b). The VERIS Community Database (VCDB). https://verisframework.org/vcdb.html

Wernerfelt, B. (1984). A resource-based view of the firm, Strategic Management Journal 5(2): 171–180. https://doi.org/10.1002/smj.4250050207

Zadeh, L. A. (1965). Fuzzy sets, Information and Control 8(3): 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X

APPENDIX A

Table A. 1 provides the list of dimensions used in fsQCA and the questionnaire questions under each of them.

Table A. 1: Construct dimensions measured in fsQCA and related questionnaire questions.

Dimensions	Related Questions
D1. Knowledge	
KDIG	Q1.1. How would you evaluate your knowledge of the digital transformation ambitions of your firm?
KCYBSEC	Q1.2. How would you evaluate your knowledge of the cybersecurity of your firm?
D2. Perception of Threats	Q2. Please rank the following immediate threats facing your facility(ies):
TFIN	Q2.1. Financial risks (e.g., inflation, recession, investment, etc.).
TOPR	Q2.2. Operational risks (e.g., operations disrupted due to strike or labor disputes).
TCYBERSEC	Q2.3. Cybersecurity risks (e.g., disruptive to building systems due to update errors or attack).
D3. Cybersecurity Preparedness	Q3. Please indicate to what extent you agree or disagree with the following statements about your firm, cybersecurity preparedness for its facilities:
CYBERSECPOL	Q3.1. Our organization has a clear cybersecurity policy.
PREPTRN	Q3.2. Our organization provides annual cybersecurity and awareness training.
PREPPOS	Q3.3. Our organization's cybersecurity training and awareness programs are conducted in a manner that promotes positive change among end-users.
PREPBMS	Q3.4. Our organization's cybersecurity policy includes building management and operations systems.
D4. Perception of Barriers	Q4. To what extent are the following aspects perceived as barriers to cybersecurity for your facilities in your firm?
BARLOI	Q4.1. Level of investment on cybersecurity awareness and preparedness.
BARRA	Q4.2. Relative advantage of cybersecurity.
BARLEG	Q4.3. Legacy systems.
BARCOMP	Q4.4. System compatibility.
BARDTMNG	Q4.5. Data management.
BARKNG	Q4.6. Employee knowledge and skills on cybersecurity.
BARMNGT	Q4.7. Top management commitment to cyber secure assets.
BARMA	Q4.8. Market (customer) acceptance.
BARTEC	Q4.9. Technology suppliers and partners.
D5. Perception of Incident Criticality	Q5. If your building is hacked, how critical would each of the following be?
CRTFINL	Q5.1. An incident results in financial loss.
CRTILOS	Q5.2. Confidential information is compromised or stolen.
CRTBR	Q5.3. The company's brand or reputation is damaged.
CRTLOC	Q5.4. The company loses customers.
CRTLOP	Q5.5. The network slows down or becomes unavailable for a period of time (loss of productivity).

CRTIP	Q5.6. Intellectual property, trade secrets or other proprietary material is stolen.
CRTSUP	Q5.7. The company loses partners/suppliers.
CRTHL	Q5.8. Human lives endangered.
CRTCS	Q5.9. Company sued.
D6. Technology Turbulence	Q6. Please indicate to what extent you agree or disagree with the following statements on technology change in FM industry:
TECHTURB1	Q6.1. Information technology in our industry changes rapidly.
TECHTURB2	Q6.2. Information technology in our industry provides opportunity.
TECHTURB3	Q6.3. A large number of new product/service ideas have been made possible through technological breakthroughs in our industry.
D7. Market Dynamism	Q7. Please indicate to what extent you agree or disagree with the following statements on market change in the FM industry:
MARKDYN1	Q7.1. In our kind of business, customers' service preferences change quite a bit over time.
MARKDYN2	Q7.2. Our customers tend to look for new services all the time.
MARKDYN3	Q7.3. New customers tend to have product-related needs that are different from those of our existing customers.
MARKDYN4	Q7.4. Customer requirements vary a lot across different customer segments.
O1. Outcome	
OUTCOME	Q8. As far as you know, has your organization ever experienced a cybersecurity incident?

APPENDIX B

Table B. 1 provides the sufficiency metrics for the 10 labelled pathways.

Table B. 1: fsQCA configuration metrics (Consistency, Coverage, PRI).

Config	Configuration label	Consistency	Raw coverage	PRI	Freq (cases with membership ≥ 0.5)
1	Unprepared Minimalist	0.545	0.212	0.166	29
2	Market-Driven Reactor	0.531	0.205	0.116	29
3	Tech-Focused Struggler	0.524	0.241	0.091	41
4	External Pressure Cooker	0.499	0.348	-0.006	95
5	Financial Fortress	0.498	0.208	-0.006	38
6	Operational Leader	0.610	0.171	0.360	10
7	Cybersecurity Champion	0.562	0.162	0.220	10
8	Well-Rounded Defender	0.616	0.126	0.378	5
9	Balanced Protector	0.560	0.123	0.215	6
10	Comprehensive Defender	0.587	0.182	0.295	26