IFMA ESPAÑA

Digital Magazine · Número especial de junio 2026

Pathways to Cyber Peril:
Cybersecurity Breaches in Facility Management

An interview with Dr Erika A. Pärn & Jeffrey Saunders

New York University Abu Dhabi · Danish National Defence Technology Centre

Published Research Citation

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

Forthcoming Book

Securing Twin Systems — Pärn & García de Soto. Available on Amazon Kindle and in print, expected late July 2026.

About the Authors

Dr Erika A. Pärn is a Research Scientist in the Division of Engineering at New York University Abu Dhabi (NYUAD) at S.M.A.R.T. Construction Research Group and a research collaborator at University of Cambridge. Her research focuses on digital twin systems and cybersecurity risk in the built environment, digital asset management, and the intersection of building information modelling and cyber resilience. This research was supported by NYUAD's Centre for Cyber Security (CCS-AD) and the SHORES centre, funded by Tamkeen.

Jeffrey Saunders is Chief Technology Officer at the Danish National Defence Technology Centre. He brings extensive practitioner experience in cyber risk management across critical infrastructure and facilities sectors. He previously served as Director of Research at IFMA, where he helped shape research and thought leadership on the future of facility management, digital transformation, workplace change, and digital risk in digitized buildings.

Prof. Borja García de Soto is an Associate Professor of Civil and Urban Engineering at New York University Abu Dhabi and a Global Network Associate Professor at NYU Tandon. He directs the S.M.A.R.T. Construction Research Group at NYUAD, where his research focuses on construction automation and robotics, digital twins for the built environment, AEC cybersecurity, AI/LLMs in construction, lean project delivery, and BIM.

Direct Quote from Prof. Borja García de Soto

“La ciberseguridad ya no es únicamente una cuestión tecnológica; es una responsabilidad estratégica de liderazgo en la gestión de instalaciones. A medida que los edificios se vuelven más inteligentes y conectados, las organizaciones deben integrar la resiliencia cibernética en su cultura, sus procesos y sus decisiones operativas desde el primer día.”

The Interview

Q1. What motivated you to conduct this research on cybersecurity breaches in facility management?

Dr. Pärn and Prof. Garcia de Soto (EP & GdS): The motivation came from a gap we (Dr. Pärn and Prof. García de Soto) kept encountering in the literature. We consistently found an alarming lack of discussion on the cybersecurity risks of the rapid digitalisation of the built environment, particularly in construction and facilities management. While cybersecurity research was flourishing in IT and critical infrastructure sectors, FM was lagging behind, both in academic attention and in organisational readiness on the ground. Facilities are becoming extraordinarily digitally complex environments, yet the sector has no comprehensive, empirically grounded map of how breaches actually happen in practice. We wanted to move beyond generic advice and give FM professionals something diagnostic and actionable. Working with IFMA to reach over 15,000 practitioners globally gave us the scale to do that rigorously.

Jeffrey Saunders (JSS): I have worked in strategic foresight since the early 2000s. In 2010, I began working with the Danish facility management company ISS on the ISS 2020 Vision series, a series of 6 white books, which explored trends shaping the future of work, workplaces, and the workforce.

One of the key megatrends we tracked was the growing use of technology in physical environments through digitisation and digitalisation. As physical assets and related processes became increasingly connected, the role of facility managers would also change. Facility managers would need to help protect organisations' digital assets as well as their physical ones.

Later, when I served as Director of Research for the International Facility Management Association, a natural research question emerged: how were cybersecurity breaches affecting the facility management profession? It was only natural to reach out to Erika and Borja, leading experts on cybersecurity in the built environment, for their help and insights.

Q2. Why is cybersecurity becoming such a critical issue for facility managers today?

EP & GdS: Facilities managers today are, in effect, custodians of vast digital ecosystems building management systems, IoT-connected HVAC and access controls, fire safety networks, energy management platforms, and increasingly, building information models and digital twins. A breach in any of these does not just mean a data leak; it can mean physical operational disruption, compromised life safety systems, or exposure of highly sensitive personal data. At the same time, FM organisations are subject to increasingly stringent data protection regulation GDPR in Europe, the CCPA in the United States, which adds legal and reputational dimensions to what was once viewed primarily as an IT problem. The attack surface has expanded enormously, and FM has not always kept pace.

JSS: As a supplement to Erika and Borja's excellent answer, I would add that facilities are becoming intelligent, connected environments that continuously collect data, automate decisions, and interact with core business systems. If those systems are compromised, the impact is not confined to the organisations networks and data; it can affect whether people can enter or occupy a building safely and whether operations can continue.

For facility managers, cybersecurity is therefore becoming part of their professional duty of care. The role is expanding from maintaining buildings to safeguarding the resilience of the environments in which people work. That requires closer collaboration with IT, risk, security, HR, and senior leadership, because the future workplace is both physical and digital at the same time.

Q3. The report highlights the importance of internal preparedness. What are the most important internal capabilities organisations should develop?

EP & GdS: Our analysis consistently pointed to three internal organisational capabilities as foundational. First, cybersecurity knowledge, not just at a senior level, but embedded across the workforce. Our data showed that employee knowledge gaps were among the most prominent barriers in the sector. Second, formal policies that explicitly cover operational technology, not just IT systems. We found that FM organisations were significantly better prepared in terms of general IT cybersecurity policies than in BMS-specific ones, a gap that is particularly dangerous because building automation systems are often the most exposed entry points. Third, incident response planning: knowing what to do when a breach occurs, not just hoping prevention will be sufficient. Preparedness is not a single switch; it is a layered organisational capability.

Figure 1 below, reproduced from the published paper (Parn et al., 2026), illustrates the seven dimensions — from knowledge and threat perception through to technology turbulence and market dynamism — whose combinations drive the ten breach configurations identified in the study.

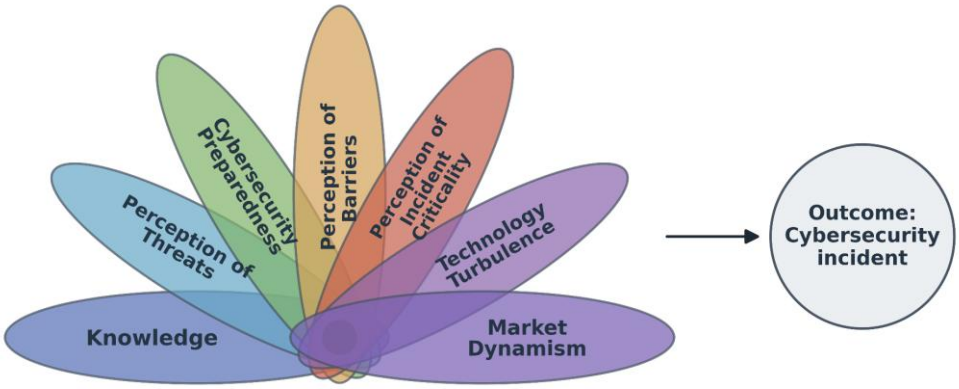

Figure 1: The seven fsQCA dimensions and their relationship to the outcome of a cybersecurity incident (Parn et al., 2026, Figure 2).

JSS: I support Erika and Borja's answer and state organisations need stronger internal coordination between facilities, IT, physical security, risk, and senior leadership. Facility managers should be asking themselves: when was the last time we had a serious conversation with IT about building systems, operational technology, access control, or connected workplace platforms? Do we have regular check-ins, where do we share responsibilities, and how do we escalate issues?

If the answer is "I can't remember" or "no," then that is a clear preparedness gap. Organisations cannot afford to manage security threats as separate IT security on one side and physical security on the other. They need an integrated enterprise security posture that recognises the workplace as both a physical and digital environment.

For facility managers, this means becoming more fluent in cybersecurity conversations and ensuring that building systems are visible within the organisation's wider risk management, governance, and incident response structures. The key internal capability is not just technical expertise; it is the ability to collaborate across silos before a breach occurs.

Q4. Your research identifies several configurations that may lead to cybersecurity breaches. Which of these did you find most concerning?

EP & GdS: The configurations we find most concerning are those labelled *Unprepared Minimalist, Market-Driven Reactor,* and *External Pressure Cooker,* the high-risk cluster characterised by an absence of internal preparedness alongside significant external pressure. These represent organisations that are being pulled along by market dynamics or technological change without having built the internal defences to cope. They are reactive rather than proactive. What makes them especially worrying is that they are not uncommon, the External Pressure Cooker configuration had the highest raw coverage of all ten pathways, meaning it captured the largest share of breach cases in our sample.

But perhaps the most intellectually striking finding was our *Comprehensive Defender* configuration organisations with strong knowledge, preparedness, and policies that still experienced breaches. This tells us that maturity alone is not a guarantee of safety. What it likely reflects is that better-prepared organisations have more sophisticated detection capabilities, so they see breaches that less mature organisations may be experiencing in silence. That is a paradox FM managers need to understand: investing in cybersecurity infrastructure increases the visibility of threats, which is ultimately a good thing, even if the reported incident count rises.

JSS: I would add that organisations need to work from the assumption that cybersecurity breaches will happen. No defence is perfect, especially as buildings, workplaces, and operational systems become more connected. The real test of preparedness is therefore not whether an organisation can prevent every breach, but whether it can limit the damage, maintain critical operations, recover quickly, and learn from the incident.

Better preparedness reduces the impact of breaches. It turns cybersecurity from a purely defensive exercise into a resilience capability.

Q5. To what extent are cybersecurity risks in facility management more organisational than purely technological?

EP & GdS: Overwhelmingly organisational. The technology dimension matters, of course, legacy systems, compatibility issues, and rapid technology turbulence all feature in our findings. But the configurations that showed the strongest breach-specificity, the clearest discrimination between organisations that experienced breaches and those that did not, were driven by internal factors: perception of operational and cybersecurity threats, organisational readiness, and the presence or absence of formal governance. Earlier research by Ghadiminia and colleagues found that FM organisations tend to over-rely on technology for cybersecurity management while neglecting the roles of people and processes. Our configurational findings confirm this pattern at scale. Culture, governance, and human awareness are not soft supplements to a technical strategy - they are the strategy.

JSS: I agree that the risks are overwhelmingly organisational, because technology only becomes secure when it is properly governed, maintained, and understood. Many vulnerabilities exist in the gaps between departments: who owns the building management system, who approves vendor access, who monitors connected assets, who updates legacy systems, and who is responsible when something goes wrong?

Those are not purely technical questions. They are questions of accountability, coordination, procurement, training, and leadership. A technically sound system can still create risk if no one knows who is responsible for it, if suppliers have unchecked access, or if facilities and IT are not working from the same risk picture.

So the issue is not whether cybersecurity belongs to IT or FM. It belongs to the organisation as a whole. The facility manager's role is to make sure the physical environment is included in that enterprise-wide view of cyber risk.

Q6. What role do knowledge gaps and lack of cyber awareness play in increasing exposure to cyber incidents?

EP & GdS: A very significant role. Knowledge-based barriers consistently emerged as among the most impactful in our analysis. Organisations where staff lacked cybersecurity awareness were poorly positioned to manage even well-understood threat types. This connects to one of our configurations directly: high technology turbulence combined with low cybersecurity knowledge creates blind spots where threats like ransomware can be introduced via phishing or unpatched software without anyone recognising the warning signs. Training and awareness programmes are not a luxury, they are a core infrastructure investment, as important as any technical control.

JSS: I would add that knowledge gaps not only increase the likelihood of a breach, they delay recognition and response. In facility management, many cyber incidents may first appear as operational anomalies. An automatic door could behave strangely, or a building management system may slow down. A vendor may display unusual access behaviors in the log data, or a sensor network could produce unexpected data. If staff do not understand the cyber dimension of these systems, they may treat these warning signs as routine technical faults rather than potential security incidents.

The longer an incident goes unrecognised, the greater the potential impact on operations and safety. Facility managers and frontline teams do not need to become cybersecurity specialists, but they do need to know what looks suspicious, who to contact, and how to escalate concerns quickly.

Q7. The report suggests that external pressures — technological turbulence and market dynamics — can increase risk when internal preparedness is weak. How should organisations respond to this?

EP & GdS: The key insight here is that external pressures are not controllable, but internal readiness is. Organisations cannot slow down the rate of technological change in their industry, nor can they opt out of competitive market dynamics. What they can do is ensure that their internal capabilities keep pace. Concretely, this means that every time a new technology is adopted , a new BMS platform, an IoT sensor network, a cloud-based FM system, or a digital twin a cybersecurity impact assessment should be part of the procurement process, not an afterthought. The Technology-Organisation-Environment framework underpinning our theoretical approach captures this well: technological and environmental pressures must be met with proportionate organisational responses.

JSS: I would add that organisations need to treat cybersecurity as part of change management. Every new technology, supplier relationship, or workplace system changes the risk profile of the organisation. The question should not only be "What value does this technology create?" but also "What new dependencies and vulnerabilities does it introduce?" Cybersecurity should be built into decision-making from the start, not added later when problems appear.

Q8. Are facility managers sufficiently involved in cybersecurity strategy today, or is this still seen mainly as an IT responsibility?

Insufficiently, in our experience. One finding from our survey that reflects this is that FM professionals often perceive cybersecurity as someone else's organisational responsibility, namely IT department's problem, or something covered by insurance. This perception is both widespread and dangerous. FM professionals manage the physical and operational systems that are increasingly targeted precisely because they sit at the intersection of operational technology and information technology, an intersection that traditional IT security frameworks were not designed to cover. FM professionals need a seat at the cybersecurity governance table, and industry bodies like IFMA have an important role to play in normalising that expectation.

JSS: Agreed.

Q9. Which assets or systems do organisations tend to underestimate when assessing cybersecurity risk?

EP & GdS: Building management and automation systems are chronically underestimated. Our data showed that while organisations scored reasonably on general IT cybersecurity policies (mean score 5.33 out of 7), BMS-specific policy coverage was notably weaker (4.66). Yet these systems, controlling HVAC, access, fire safety, energy management, can be weaponised to cause physical operational disruption in ways that go well beyond data theft. Digital twins are an emerging concern in the same vein: as FM organisations create high-fidelity virtual replicas of their physical assets, those models become extremely sensitive targets, both as intelligence sources during reconnaissance for attackers and as control interfaces if compromised. Our forthcoming book, Securing Twin Systems, addresses precisely this challenge. Supply chain and partner interfaces are also underestimated; the relationships between FM organisations and their technology suppliers and subcontractors represent significant exposure points that often receive insufficient scrutiny.

Q10. What practical first steps would you recommend to FM teams wanting to improve their cybersecurity readiness?

EP & GdS: Three immediate priorities. First, conduct an honest inventory of all connected systems in your facilities, not just IT assets, but every BMS component, IoT device, digital twin interface, smart device, and third-party connection. You cannot protect what you have not mapped. Second, review whether your cybersecurity policy explicitly covers operational technology and building systems, not just corporate IT. If it does not, close that gap. Third, invest in awareness training across the whole organisation. The data consistently shows that human knowledge gaps are among the most consequential vulnerability factors. These steps cost relatively little but address the most common configurations we identified as high-risk.

JSS: I would add a fourth step: FM'ers need to engage with their counterparts in their organisation and key suppliers. FM teams should sit down with IT, physical security, procurement, risk, and key suppliers to clarify who is responsible for what. Many vulnerabilities arise not because no one cares, but because ownership is unclear.

A simple first exercise is to ask: who monitors our connected building systems, who can access them, who approves updates, who manages suppliers, and who is contacted if something looks wrong? If those answers are unclear, then the organisation has already identified a readiness gap.

Improving cybersecurity readiness does not have to start with a major investment. It can start with better coordination, clearer accountability, and regular conversations across the teams that share responsibility.

Q11. How do you see the relationship between smart buildings, digital transformation and cybersecurity evolving over the next few years?

EP & GdS: The risk surface will continue to expand. As individual buildings connect to micro-grids, smart neighbourhoods, and ultimately smart city infrastructure, the interdependencies multiply, and so do the potential vectors for attack. AI-driven building automation, digital twins, and cloud FM platforms all introduce capabilities that are genuinely valuable, but each represents a new attack surface if not secured from the outset. Digital twins in particular deserve special attention: they create persistent, data-rich representations of physical infrastructure that, if compromised, could give an attacker a detailed operational intelligence picture of a facility before any physical intervention. This is precisely the subject of our forthcoming book, Securing Twin Systems, which will be available on Amazon Kindle and in print by late July 2026. The research agenda for the field is clear: we need longitudinal studies that track how these configurations evolve as FM systems become more autonomous and more integrated.

JSS: As Erika and Borja argue, cybersecurity will be a design condition for smart buildings, not a separate technical layer added afterwards. As buildings become more adaptive, data-driven, and integrated with wider urban systems, trust will become central to their value. A smart building that cannot be trusted is not really smart; it is a liability.

Successful FM organisations will not treat digital transformation and cybersecurity as competing priorities. They will understand that secure systems are what make digital transformation of facility management sustainable.

Q12. What message would you like to share with IFMA Spain members regarding cybersecurity and operational resilience?

EP & GdS: Cybersecurity is not solely an IT department problem, it is a facilities leadership problem. The organisations in our study that were most resilient were not necessarily those with the largest budgets; they were those where cybersecurity awareness was embedded in culture, where governance structures assigned clear responsibility, and where people at every level understood what was at stake. IFMA members are custodians of critical infrastructure. The physical and digital fabric of the built environment, including its growing layer of digital twin representations, depends on the decisions you make about how to manage these risks. The good news is that the pathways to vulnerability are knowable. Our research has mapped ten of them. That means the pathways to resilience are equally within reach. Act on them before a breach does it for you.

JSS: My message is simple: do not wait for a breach before making cybersecurity a priority. Facility managers now work at the intersection of buildings, people, data, technology, and business continuity. That gives the profession a strategic role in operational resilience.

For IFMA Spain members, the opportunity is to lead this conversation internally. Ask whether building systems are part of the wider cybersecurity strategy, whether facilities and IT share the same risk picture, and whether teams know how to respond when connected systems behave abnormally. Resilience starts with those questions, before a breach forces the issue.

Full Citation

Published Research Citation

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

Forthcoming Book

Securing Twin Systems: Cybersecurity and Digital Twins in the Built Environment — Pärn & García de Soto. Available on Amazon Kindle and in print, expected late July 2026.