MIS Quarterly Executive

Volume 23 | Issue 4 Article 6

December 2024

Identifying and Filling Gaps in Operational Technology Cybersecurity

Abbatemarco Nico

Hans Brechbühl

MIS Quarterly Executive

Identifying and Filling Gaps in Operational Technology Cybersecurity

Recent advancements in digital technologies have significantly reshaped operational technology (which consists of the hardware and software that monitor and control industrial assets and processes). The increased connectivity of these devices introduces cybersecurity risks that were once unheard of. Much like in the IT domain, ensuring robust cybersecurity in operational technology goes beyond technical solutions—it also hinges on specific organizational factors. Drawing on insights from 36 leaders across 14 global corporations, we identify critical gaps in these areas and provide recommendations to bridge them.[1,2]

Abbatemarco Nico
SDA Bocconi School of Management (Italy)

Hans Brechbühl
SDA Bocconi School of Management (Italy)

Operational Technology Cybersecurity Poses a Significant Challenge

Operational technology (OT) refers to hardware and software systems, such as programmable logic controllers (PLCs), distributed control systems (DCS), and supervisory control and data acquisition (SCADA) systems, used to monitor and control physical assets and processes in industries like manufacturing, energy and utilities. Historically, OT environments had little to no connection to external networks, so cybersecurity was rarely a primary concern. However, with the rise of "Industry 4.0" and similar initiatives, traditional OT systems are increasingly being connected to the internet and integrated with modern digital solutions. These initiatives are reshaping the OT landscape, bringing both operational advantages and heightened cybersecurity risks.

The Industry 4.0[3] concept originated in Europe and involves the adoption of a wide range of digital technologies, such as the Internet of Things, cloud computing and edge computing, for use in OT applications. These applications enable features such as process integration and real-time information sharing, which can drive key performance objectives[4] like enhanced

1 Stuart Madnick is the senior accepting editor for this article.

2 The authors thank Stuart Madnick and the members of the review team for their valuable feedback throughout the review process. A special thanks is also due to the production editor, David Seabrook, and the editor-in-chief Iris Junglas for their insightful guidance. We gratefully acknowledge the support of all the industry experts who were involved in this initiative and their respective companies. Their contributions were crucial for the success of this work.

3 For an introduction to Industry 4.0, see Lasi, H., Fettke, P., Kemper, H.-G., Feld, T. and Hoffmann, M. "Industry 4.0," *Business & Information Systems Engineering* (6:4), June 2014, pp. 239-242.

4 For an overview of potential performance improvements offered by Industry 4.0 initiatives, see Dalenogare, L. S., Benitez, G. B., Ayala, N. F. and Frank, A. G. "The Expected Contribution of Industry 4.0 Technologies for Industrial Performance," *International Journal of Production Economics* (204), October 2018, pp. 383-394.

DOI: 10.17705/2msqe.00105

transparency and greater flexibility. Indeed, the potential benefits of Industry 4.0 projects range from incremental productivity improvements to radical business model shifts like "servitization."[5] These benefits can be crucial for an industrial company's survival in an economy that increasingly favors value-added products—especially those incorporating digital services—over purely physical goods. As a result, the risks of missing out on Industry 4.0 or equivalent initiatives are significant.

Despite the myriad benefits promised by Industry 4.0, numerous initiatives have stalled or been abandoned altogether. As highlighted by various studies in recent years, one of the obstacles linked with these failures is the difficulty of addressing cyber risks in OT environments.[6]

Today, addressing cyber risks is one of the key challenges for public and private organizations worldwide, regardless of industrial sector, geographical location or size. The challenge is even greater for companies whose core business units have a low level of digital literacy and, as a consequence, have a limited capability of managing cyber risks in their domain of expertise. This is often the case for OT professionals in different organizational functions.[7]

By amplifying the role and reach of digital technologies in OT contexts, Industry 4.0 initiatives have further exacerbated cyber risks.[8] Mitigating cyber risks is particularly challenging in these contexts for several reasons, including, but not limited to:

- The increase of potential cyberattack targets due to the proliferation of internet-connected devices on the factory floor[9]
- The emergence of cyber-physical threats[10]
- Weaknesses in outdated industrial systems, which often lack proper cybersecurity support.[11]

It is no coincidence that, in recent years, there has been a significant increase in cyberattacks targeting companies in the manufacturing sector. Various industry reports[12] indicate a 100-150% surge in cyberattacks in 2022 compared to the previous year, with most being ransomware attacks and over 65% of the publicly disclosed attacks targeting the manufacturing sector. Attacks aimed at manufacturing companies often have objectives beyond mere extortion, such as the direct sabotage of industrial systems.[13] A notable example is the NotPetya malware, which initially masqueraded as ransomware but was primarily intended to disrupt the operations of the affected company.[14]

Regardless of their type, OT cyberattacks may cause significant disruptions to operations and result in substantial financial losses. On average, the cost of a cyber breach in the manufacturing industry ranges from $3 million to $7 million per incident, with the disruption of operations lasting an average of four days.[15]

5 Servitization refers to delivering customer-centric outcomes through business model innovation. For a review of servitization and related concepts, see Kowalkowski, C., Gebauer, H., Kamp, B. and Parry, G. "Servitization and Deservitization: Overview, Concepts, and Definitions," *Industrial Marketing Management* (60), January 2017, pp. 4-10.

6 See, for example: 1) Abbatemarco, N., Meregalli, S. and Gaur, A. "Stuck in Pilot Purgatory: Understanding and Addressing the Current Challenges of Industrial IOT in Manufacturing," *Proceedings of the 55th Hawaii International Conference on System Sciences*, January 2022, pp. 6871-6880.

7 For more about digital literacy in evolving operational technology contexts, see Tripathi, S. and Gupta, M. "A Holistic Model for Global Industry 4.0 Readiness Assessment," *Benchmarking: An International Journal* (28:10), March 2021, pp. 3006-3039.

8 See, for example, Culot, G., Fattori, F., Podrecca, M. and Sartor, M. "Addressing Industry 4.0 Cybersecurity Challenges," *IEEE Engineering Management Review* (47:3), July 2019, pp. 79-86.

9 See, for example, Chhetri, S. R., Rashid, N., Faezi, S. and Al Faruque, M. A. "Security Trends and Advances in Manufacturing Systems in the Era of Industry 4.0," *Proceedings of the 36th IEEE/ACM International Conference on Computer-Aided Design*, November 2017, pp. 1039-1046.

10 See, for example, He, H. and Yan, J. "Cyber-Physical Attacks and Defences in the Smart Grid: A Survey," *IET Cyber-Physical Systems: Theory & Applications* (1:1), December 2016, pp. 13-27.

11 See, for example, Lee, S., Lee, S., Yoo, H., Kwon, S. and Shon, T. "Design and Implementation of Cybersecurity Testbed for Industrial IoT Systems," *The Journal of Supercomputing* (74:20), September 2018, pp. 4506-4520.

12 See, for example, *OT Cybersecurity Year in Review*, Dragos, 2023, available at https://www.dragos.com/year-in-review/.

13 For more information about potential types of cyber-harm, see Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. and Upton, D. "A taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate," *Journal of Cybersecurity* (4:1), October 2018, pp. 1-15.

14 For an overview of NotPetya, see Greenberg, A. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED, August 2018, available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

15 For an updated perspective on data breaches, see IBM. *Cost of a Data Breach Report*, IBM, 2023, available at: https://www.ibm.com/reports/data-breach.

As these examples illustrate, securing OT systems is critical, as a cyberattack is often capable of slowing down or completely halting an organization's industrial processes. Adopting robust cybersecurity solutions has therefore become a critical imperative for industrial organizations, mandated by both resilience[16] and compliance[17] needs. However, the implementation of such solutions is a challenging task.

Focus of Our Research

In this article, we identify the cybersecurity gaps that industrial companies have in their operational technology and provide recommendations for filling them. We also highlight the differences between OT cybersecurity and information systems cybersecurity.[18]

Our starting point was to identify the organizational conditions, beyond technical performance, that determine the successful implementation of cybersecurity for OT devices. It is important to clarify that our emphasis on organizational aspects does not assume that mature and widely adopted technological solutions for securing OT devices are available. In fact, one of the primary challenges in this domain relates to the difficulty of applying cybersecurity measures in a standardized fashion in companies that may have very different digital configurations, as often happens in manufacturing plants. However, real-world evidence suggests that the primary obstacles in establishing OT cybersecurity are organizational rather than technical. For example, a recent survey[19] involving 500 global manufacturing companies revealed that despite the importance of cybersecurity, merely 50% consider OT cybersecurity to be significant in their overall risk assessment.

To identify the conditions for success of OT cybersecurity, we turned to the concept of "technochange,"[20] a widely recognized framework for analyzing technological projects that cause significant organizational change, not just from an IT perspective but also taking account of the complementary shifts needed in organizational structures, work processes and cultural practices. In addition to a functional solution (along with its support system) and effective project management, the technochange concept identifies three additional conditions for the success of such projects: completeness, alignment/implementability and the ability to capture benefits. These success conditions indicate the organizational complexities that need to be navigated to achieve project success. (Appendix B provides more information about technochange and how the concept can be applied to OT cybersecurity.)

To explore how managers navigate the organizational complexities hindering the implementation of a cybersecure OT environment, and thus identify the gaps in their OT cybersecurity, we ran a series of focus groups between February 2022 and June 2023. Focus group participants included 36 industry experts from 14 large global companies, including chief information officers, chief information security officers (CISOs) and leaders of OT initiatives. (The sectors represented by the 14 companies were manufacturing (4), food processing (3), chemicals (2) and one each from logistics, energy, oil and gas, textile and construction. (Appendix A lists the focus group participants for each of the 14 companies and describes the data collection and analysis methods we used following the focus groups.) Each participating company had annual revenues exceeding $1 billion, more than 5,000 employees, a global footprint and an ongoing Industry 4.0 or equivalent initiative (started at least one year before the first focus group). All the participants had been involved or were currently involved in at least one such initiative.

16 Resilience is the capacity to effectively respond to and recover from cyber incidents. See Onwubiko, C. "Focusing on the Recovery Aspects of Cyber Resilience," *Proceedings of 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, 2020, pp. 1-13.

17 Examples include compliance with the EU's Network and Information Security Directive (NIS) and its upcoming updated version (NIS2).

18 For an overview of how securing OT devices differs from securing IT systems, see *IT vs OT Security: Key Differences in Cybersecurity*, Claroty Blog, June 13, 2023, available at: https://claroty.com/blog/it-and-ot-cybersecurity-key-differences#:~:text=One%20of%20the%20main%20differences,control%20physical%20processes%20and%20systems.

19 *2022 State of Operational Technology and Cybersecurity Report*, Fortinet, 2022, available at https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf.

20 See Markus M. L. "Technochange Management: Using IT to Drive Organizational Change," *Journal of Information Technology* (19:1), March 2004, pp. 4-20.

Identifying the Gaps in Operational Technology Cybersecurity

Focus group participants identified two major challenges that hinder OT cybersecurity. First, there is the limited familiarity of OT personnel with digital technologies, leading to a low level of cyber awareness. This results in a lack of understanding of the existing cyber challenges and difficulties in communicating effectively with IT and cybersecurity specialists and in aligning security priorities with a unified perspective.

Second, the cybersecurity team typically lacks authority outside the conventional IT domain. This can be largely attributed to CISOs often holding a lower-tier C-level position despite bearing responsibilities that exceed their rank. As a result, there is a discrepancy between the designated role of the CISO and their capacity to tackle cybersecurity challenges in an OT context. In addition, external factors such as the shortage of skilled cybersecurity personnel exacerbate these challenges. Below, we detail how these challenges and factors impact the three conditions for success in the context of OT cybersecurity.

Gaps in the Completeness Success Condition

Completeness ensures that cybersecurity is workable, meaning it is strategically positioned to create value for the organization. Among the focus group participants, completeness was lacking due to four main reasons.

Cybersecurity Only Done at the Very End of an OT Project. In general IT projects, cybersecurity may become an afterthought due to an emphasis on functionality and delivery speed, resulting in last-minute cybersecurity implementations. However, the cybersecurity team is typically aware of new IT projects and can at least advocate the need for early involvement to mitigate risks.[21] In OT initiatives, however, the project team typically operates within a specific context (e.g., a region or a single plant) and this can, either intentionally or unintentionally, limit interactions with the (usually more) centralized cybersecurity team. Frequently, OT project leaders give the cybersecurity team an ambiguous assurance that cybersecurity measures will, in the words of the CISO at Food Processing Company 1,[22] be "bolted on afterwards." As a result, CISOs need to catch up once the project is already underway or nearing completion. This situation can easily lead to an endless loop of back-and-forth between the project and cybersecurity teams, as described by the energy company's strategy and planning manager: "We would get a new app and send it to the security team. They would say, 'Wow, this is very insecure,' and send it back, which would create tension between teams and was very inefficient."

Cybersecurity Team Having No Real Power or Support: In the IT domain, cybersecurity teams may lack sufficient authority to enforce policies or make decisions due to organizational silos or to top management underestimating the importance of cybersecurity. However, the role and importance of the CISO are generally recognized (and growing) in IT, especially following recent cyber regulations.[23] But in OT initiatives, project teams frequently do not regard the CISO as a top manager and may even be unaware of the cybersecurity team's role, resulting in limited authority and influence for the security team and a lack of involvement in the initiative. As mentioned by the CIO of Chemicals Company 1, this deficiency often stems from a lack of cybersecurity expertise among executive teams: "The executive team thought we were fine, and there was absolutely no view into OT at all. I came in and said 'We have a big problem.' At first, there was no appreciation for the risk: 'We're not a bank; why would anyone want to attack us?'"

This lack of power results in the cybersecurity team paradoxically not having a voice in certain crucial decisions regarding the cyber risk to OT initiatives. As noted by the CIO of Manufacturing Company 4, if the cybersecurity team has little to no authority, OT personnel tend to postpone security actions: "The business units always wanted to delay: one more year, one more year..."

21 See Weir, C., Migues, S. and Williams, L. "Exploring the Shift in Security Responsibility," *IEEE Security & Privacy* (20:6), November 2022, pp. 8-17.

22 All quotes are from focus group participants. The 14 anonymous companies, together with the roles of their participants, are listed in Appendix A.

23 See Karanja, E. "The Role of the Chief Information Security Officer in the Management of IT Security," *Information & Computer Security* (25:3), July 2017, pp. 300-329.

As emphasized by the Energy Company's IT director, the situation is particularly critical when the IT unit and cybersecurity team are expected not only to manage, but also own the risks:"The approach is unsustainable in the long term, especially when you have server owners and asset owners, and the accountability is put on them."

This lack of power can also affect other departments indirectly involved in an OT initiative. For instance, the Oil and Gas Company's cybersecurity director highlighted a situation that may arise when the cybersecurity team lacks the authority to insist that the procurement unit include specific clauses as part of the vendor selection process. This company had chosen a vendor that did not allow direct application of publicly available security patches, such as Windows updates for its Windows-based devices. The cybersecurity director said:

> *"We also found some vendors that say, OK, I know there's a Windows patch available, but I do not authorize you to put that patch directly. So that's a tough situation because you have to take the risk. … If you have two similar solutions, you should not only look at the functional aspects, but also at how you can sustain them over time."*

Underbudgeted Cybersecurity: Budget allocations for cybersecurity in many IT projects may be insufficient due to competing investment priorities. In OT initiatives, however, cybersecurity budget constraints can be even greater due to a lack of understanding of the risks and no security-specific budget. The Oil and Gas Company's CIO/CDO (chief digital officer) said that the distribution of funds often becomes "entangled in the web of organizational politics," necessitating a clear definition of accountability for budget decisions. It may not be immediately obvious to top managers that OT cybersecurity warrants additional budgetary considerations: Applying cybersecurity in an OT context might seem like merely extending the same state-of-the-art solutions used in other organizational domains, but this is a misconception.

As described earlier, the technical demands of OT cybersecurity are markedly distinct from the purely IT domain. IT projects can often benefit from certain economies of scale because they leverage common platforms that are used for various purposes (e.g., multiple SaaS applications based on the same cloud deployment). Similarly, once cybersecurity requirements are established for the main platform, they can be more easily applied across multiple other projects.

On the contrary, a typical OT scenario involves operational technology systems operating on outdated, unsupported IT systems, which require tailored monitoring solutions (as reported by the CISOs of manufacturing Companies 1 and 3, and the cybersecurity director of Food Processing Company 2). As a result, OT environments may miss out on cybersecurity economies of scale due to their greater variety. Finally, the integration of cybersecurity measures in operational technology may require a resource-intensive phased implementation to avoid disruptions.

Understaffed Cybersecurity Team: The shortage of skilled personnel is one of the key obstacles to implementing cybersecurity in IT systems, with market analyses consistently revealing a significant shortfall in qualified cybersecurity professionals.[24] However, the issue is more pronounced in operational technology, where cybersecurity experts familiar with OT initiatives are especially in short supply. The difficulty in recruiting experts with both skill sets is well-recognized, and focus group participants expressed concerns about being severely understaffed in the area of cybersecurity. Even if appropriate experts can be found, there is also the problem of retention. Younger people, who are more likely to possess the right mix of skills, are particularly challenging to retain in the face of attractive offers from large tech firms.

Gaps in the Alignment Success Condition

Alignment (also referred to as implementability) ensures that a cybersecurity solution is working—i.e., it is adopted and used throughout the organization. The organizations represented in our focus groups had gaps in this success condition due to two main reasons: misaligned priorities and the misfit between IT unit/cybersecurity teams and the OT teams, leading to a lack of coordination.

24 See, for example, *The Cybersecurity Skills Gap is a Real Threat—Here's How to Address It*, World Economic Forum, May 2, 2023, available at https://www.weforum.org/agenda/2023/05/the-cybersecurity-skills-gap-is-a-real-threat-heres-how-to-address-it/.

Misaligned Priorities: In IT projects, business units and cybersecurity teams may have differing priorities, with the former focusing on functionality and speed and the latter emphasizing security and stability. Generally speaking, however, business units can tolerate scheduled downtimes for updates, maintenance and upgrades of IT systems without significantly impacting business operations. But in OT systems, balancing the need for control desired by the cybersecurity team and the need for productivity desired by the OT team can be more challenging, as cybersecurity activities may require a partial or complete stoppage of operations. OT personnel prioritize efficiency and uptime and may view cybersecurity measures as potential hindrances.

Patch management, one of the most common cybersecurity activities in the OT domain, provides a particularly good example of this conflict. On the one hand, the IT unit and cybersecurity team want new patches to be applied promptly because any unresolved vulnerability is a potential entry point for malicious actors. On the other hand, applying patches is particularly resented by OT personnel, especially in facilities operating 24/7. In the words of the Oil and Gas Company's cybersecurity director, any stoppage required for patch application "reduces production value."

In some cases, the cybersecurity team may be unaware of the issues caused by stoppages for updates and patches. This lack of awareness, combined with the proliferation of cyber regulations in recent years, has led some of the focus group companies to adopt a questionable compliance-first approach to cybersecurity. As illustrated by the OT digital transformation director of Food Processing Company 2, this type of approach may prove especially unsuccessful in OT settings:

> *"Sometimes I go in [the factory] and they've got a vending machine that distributes gloves that they can't connect and use due to cybersecurity reasons. Where's our risk, really? As opposed to that, I've got machines that probably have the secret sauce to our core business. There's a difference in the risk profile, but sometimes it feels like the guy on the other end of the phone is just reading a policy sheet. … Most of the plant people don't trust a person who doesn't understand what's really going on."*

Misfit Between Employees Leading to Lack of Coordination: An organization's IT, security and business unit silos can hinder effective communication and collaboration in IT projects. The IT unit and cybersecurity teams are often perceived as isolated from the mainstream business processes and considered back-end functions that merely keep things running. The Logistics Company's CISO used the analogy of IT being seen as "the plumbing that just kind of does stuff." In general, IT projects predominantly involve IT professionals who often share similar working profiles and mindsets.

Conversely, OT initiatives require close collaboration between IT and OT professionals with very different profiles, including engineers, operations managers and maintenance staff. In many cases, this misfit contributes to OT, IT and cybersecurity professionals not collaborating enough during an OT project, resulting in a communication breakdown and conflicts over problem-solving approaches. As a consequence, the IT unit and cybersecurity team are often unaware of the specifics of the OT context, while OT personnel ignore the cybersecurity imperatives, further contributing to the overall misalignment of their priorities. As observed by the CIO of Manufacturing Company 1, "As long as it's a battle, you're not mature."

Gaps in the Ability to Capture Benefits Success Condition

The ability to capture benefits ensures that cybersecurity is worked—i.e., its potential benefits are actually turned into measurable organizational results. Focus group participants identified that the main reason for the gaps in this success condition is the difficulty in recognizing the tangible benefits of cybersecurity

Tangible Benefits Are Hard to Recognize: Focus group participants said that recognizing the benefits of cybersecurity posed a tough challenge. In fact, such benefits are often scarcely visible, making it difficult to justify expenditures: When the solution functions correctly, operations continue seamlessly; negative consequences only become evident when it fails. Addressing this challenge is somewhat more straightforward in

Table 1: Reasons for Gaps in the Success Conditions and Differences Between IT and OT Initiatives

Success Condition	Reasons for Gaps in OT Cybersecurity	Differences Compared to IT Cybersecurity
Completeness (Workable Solution)	Cybersecurity only done at the very end	• Cybersecurity team lacking visibility on OT initiatives • OT personnel unaware of cybersecurity requirements
	Cybersecurity team having no real power or support	• Cybersecurity team being invisible outside IT • Cybersecurity team lacking effective power outside IT
	Underbudgeted cybersecurity	• Cybersecurity team lacking effective power outside IT • OT personnel unaware of cybersecurity risks (and potential benefits) • Higher variety of OT environments
	Understaffed cybersecurity team	• Lack of personnel with knowledge in both the OT and cybersecurity domains
Alignment/ Implementability (Working Solution)	Misaligned priorities	• Cybersecurity team lacking knowledge of OT priorities • OT personnel unaware of cybersecurity risks (and potential benefits)
	Misfit between personnel leading to lack of coordination	• Different mindset between OT and IT professionals
Ability to Capture Benefits (Worked Solution)	Tangible benefits are hard to recognize	• OT personnel unaware of cybersecurity risks (and potential benefits)

conventional IT projects because the primary asset to protect is typically data, and it is easier to see how cybersecurity can help maintain data confidentiality, integrity and availability.

Conversely, cybersecurity in an OT context emphasizes the protection of physical processes and the safety and reliability of critical operations. Though today's cyber threats can have physical consequences, such as equipment damage, safety hazards or system shutdowns, OT personnel are often unaware of these threats and therefore more resistant to adopting the necessary cybersecurity measures. The challenge is further complicated by the fact that for proper risk quantification exercises,[25] OT teams need to have detailed asset management inventories. Preparing these inventories is not only time-consuming but also often perceived as adding little value.

Summary of the Gaps in the Three Conditions for Successful Operational Technology Cybersecurity

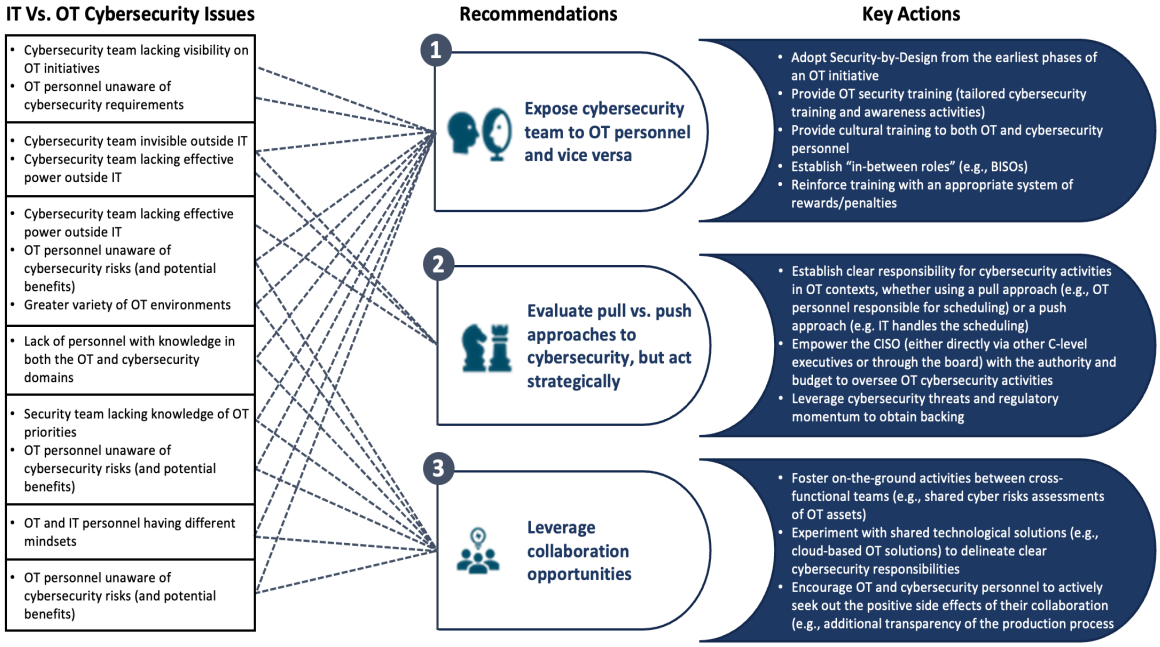
Table 1 provides a summary of the reasons for the gaps in the three conditions for success and outlines the key differences between IT and OT initiatives.

Recommendations for Filling the Gaps in Operational Technology Cybersecurity

As described above, the gaps in the success conditions identified in our focus groups clearly indicate that a successful cybersecurity program for OT initiatives is no easy task. Nonetheless,

25 For information on risk-based approaches to cybersecurity, see Boehm, J., Curcio, N., Merrath, P., Shenton, L. and Stähle, T. *"The Risk-Based Approach to Cybersecurity,"* McKinsey, October 2019 available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity.

Figure 1: Summary of the Recommendations



discussions among the participants uncovered several approaches to filling these gaps, which we have distilled into three recommendations for CIOs, CISOs and other leaders embarking on OT projects. Though these recommendations are partly applicable to IT projects, we believe that they are uniquely valuable for OT initiatives. Figure 1 summarizes the recommendations and illustrates how they help to fill the gaps in OT cybersecurity identified above.

Recommendation 1. Expose Cybersecurity Team to Operational Technology Personnel and Vice Versa

The completeness success condition requires work to be reorganized in new ways to take advantage of the benefits promised by the cybersecurity solution. To be complete, a cybersecurity solution must first be integrated into the OT initiative from the outset. This requirement is not unique to OT projects and is commonly referred to as "Secure by Design."[26] With this approach, cybersecurity is placed at the forefront of an OT (or IT) project, requiring solution developers to work closely with cybersecurity personnel, security architects and engineers in vulnerability management as they redesign the particular business processes. In the context of OT initiatives, the primary focus should be on "covering"—for example, giving the cyber team the opportunity to secure a new OT device/solution before this is added to a production line—and testing the early stages of solution development, using a security approach commonly referred to as "shifting left."[27]

Completeness also means bridging the cultural divides that exist between OT, IT and cybersecurity personnel. In particular, OT personnel must have a foundational level of cybersecurity knowledge if they are to comprehend the cyber risks that could significantly impact their operations. Most

26 For information, see *Secure by Design*, Cybersecurity & Infrastructure Agency, available at: https://www.cisa.gov/securebydesign.

27 Shift-left testing is an approach to software and system testing in which testing is performed earlier in the lifecycle. For more information, see *Shift-Left Testing*, Wikipedia, available at https://en.wikipedia.org/wiki/Shift-left_testing.

focus group participants reported mandatory annual cybersecurity training for their entire workforce. In addition, targeted cybersecurity training—such as personalized discussions for OT executives and managers on specific cyber risks unique to their field—might further enhance their awareness. Historically, these employees have been less involved in cybersecurity initiatives, and specialized training, tailored to their level of seniority and responsibility, could motivate them to take a proactive stance as they increasingly find themselves "at the heart of such initiatives" (cybersecurity director, Food Processing Company 2). As the CISO of Manufacturing Company 1 reported:

> *"When we first started our OT security program, we sent a couple of engineers to class at Idaho National Labs, where they got to do hands-on attack and defend of OT systems. That experience got them to buy in and understand the risk. More recently, as we've developed OT security centers, we made sure to target training at our people in our plants who buy and support OT equipment."*

However, in addition to technical training, bridging the cultural divide also requires cultural change, which should be a two-way effort. For OT personnel, cultural training should focus on changing their adversarial perception of IT and cybersecurity specialists, seeing them as a supportive role instead. The Energy Company's strategy and planning manager suggested the key message for this part of the training should be: "If you build it this way, you can still have autonomy, but also ensure security." A "humble" approach from IT and cybersecurity personnel can facilitate this shift in perception.

Focus group participants said that cultural change programs should be reinforced by rewards and/or penalties related to cybersecurity that are embedded in HR policies. Though participants recognized the importance of such mechanisms, there was no consensus on which of the two is more impactful. Some preferred penalties. The CIO of Chemicals Company 1 said that penalties—including firing—can help raise the general level of participation in corporate cybersecurity initiatives: "When we started reporting back to management teams, "Here are your repeat offenders, the next steps are penalties on performance and money"—that's when we got a direct correlation to improved performance on phishing campaigns."

Others provided a contrasting view, less focused on punitive measures and more on rewards for engaging in cybersecurity training. Their companies' aims are to motivate employees without intimidation, thus reducing the cultural gap between them and the cybersecurity team. Strategies for achieving this include the establishment of informal roles such as that of "cyber champions"—people recognized as having done something great in cybersecurity—or, as the CIO of Food Processing Company 1 reported, appointing Business Information Security Officers (BISOs) who act as mediators between the cybersecurity team and the business unit—in every company plant.

Conversely, IT and cybersecurity personnel must also embrace a cultural transformation to effectively collaborate with OT specialists. The former need to understand that the OT mindset prioritizes production and requires quicker responses than those typical of users of IT solutions. The CISO of Chemicals Company 1 provided this example:

> *"We have one set of service level agreements (SLAs) for firewalls in IT. We had to establish a whole separate set of SLAs for the firewalls that separate manufacturing from the rest of the network, and they're actually faster SLAs. They're sharper, stricter SLAs. On [the OT] side, … if they're asking us for a firewall change, [more often than not] it's because something is broken. The vendor is on site, can't get to what they need to get to, and if we don't get it back up in the next 20 minutes and open up a particular communication port, the vendors will be just sitting there charging however many hundred dollars an hour. And in the meantime, production is down."*

To facilitate this type of cultural change, it can be useful for cross-functional teams to work physically together rather than merely collaborating online.

Recommendation 2. Evaluate Pull Vs. Push Approaches to Cybersecurity, but Act Strategically

With the increasing adoption of cloud-based OT initiatives, activities such as patch management will become even more of a challenge. Organizations can adopt either a pull or push approach to address it.

Pull Approach: Some of the focus group organizations had tilted the balance of cybersecurity activities in favor of operational technology. The reasons for this choice include not only productivity concerns but also factors such as OT personnel's better understanding of the systems, a commitment to minimize conflicts and the need to adapt the scheduling of cybersecurity activities to the technology of individual plants (as reported by the CISO of Food Processing Company 3, and the Energy Company's cybersecurity manager and digital transformation manager). In companies adopting this approach, a conventional countermeasure to ensure that cybersecurity vulnerabilities are not completely overlooked is to establish an on-site vulnerability management team at the plant. This team is tasked with negotiating reasonable schedules that suit both OT and cybersecurity personnel and that can be tailored for each specific plant. The CISO mentioned above emphasized that the pull approach is valuable "especially for factories that are running 24/7."

Push Approach: Other focus group companies had opted to shift the balance of cybersecurity activities toward the IT unit and the cybersecurity team. The primary driver for this approach is the urgency of securing OT systems without being delayed by factory floor personnel, who might indefinitely defer action. Understandably, countermeasures are also needed for this push approach. One such strategy was described by the CIO of Manufacturing Company 4:

> *"We reached the point of thousands of obsolete devices, and finally our CEO said 'Enough, we're centralizing it all, and IT is going to drive it.' … We worked in our factories and said: 'Mainly because of cyber, we have to keep this stuff maintained. And when we do, you will have an outage.' They understand it's coming; it's communicated and scheduled for the whole year. We do it on the weekends, just every month, and we patch whatever needs to get patched in that environment in that window."*

As the Energy Company's OT digital transformation manager pointed out, the rollout of more cloud-based OT solutions will result in more centralization, likely requiring reliance on a centralized push approach to cybersecurity activities. In the meantime, either approach can be effective, provided the activities are clearly scheduled from the outset and the boundaries are explicitly defined (e.g., the IT unit must communicate and properly schedule activities even in the case of a push approach).

Acting Strategically: Both the push and pull approaches may not be limited to cybersecurity activities alone, but also influence strategic cybersecurity decisions. For example, OT personnel and the cybersecurity team might have drastically different views on how to resolve ransomware attacks. On the one hand, OT personnel might lean toward paying the ransom, considering it cost-effective compared to facing prolonged manufacturing downtimes. On the other hand, the cybersecurity team usually enforces policies against this option, arguing that paying up does not guarantee the incident will be resolved and, even worse, that there is a very high likelihood of incurring legal sanctions.

However, a necessary condition for both approaches is that the CISO, either directly or at least through the CIO, should be empowered to enforce certain directives within the OT domain. The CIO of Food Processing Company 2 clearly explained what the role of the IT unit and cybersecurity team should be in OT initiatives: "We can't own everything everywhere, but we create processes, procedures, guidelines, architecture—so that the businesses believe in them, or we're not going to get where we need to go."

Various approaches emerged in the focus groups to address the need for role alignment. For example, the Energy Company had established a policy empowering the CISO with the authority to do everything necessary to ensure cybersecurity risk was consistent with the company's risk appetite. This led it to consider entirely segregating the cybersecurity team from the IT unit to ensure adequate independent risk

assessment, exert pressure on the IT unit and prevent cybersecurity from being overshadowed by broader IT priorities. The company ultimately decided against a complete separation but empowered the CISO through direct reporting to the board and giving him independent financial authority.

From the focus group discussions, the effectiveness of the CISO and the cybersecurity team seems to be inextricably linked to getting the proper budget for cybersecurity activities and the backing of the top management. Paradoxically, the sharp rise in cyberattacks—particularly against companies with significant OT operations—has focused CEOs' minds on the need for CIOs and CISOs to be given the necessary budgets and authority, as recounted by the CIO of Manufacturing Company 4:

> *"We had a couple of cyber incidents that could have been catastrophic if we didn't catch and address them. This went all the way up to the CEO and the board. We then did a cyber simulation with our senior leaders and [a consulting company], and they kept saying OK, imagine these plants are infected. It's spreading this way and this way, and I could see them being like, 'Oh my God, this could bring us to our knees.' And once they dealt with some of that education, they were like 'do everything, … do whatever you got to do to keep us safe.'"*

If there is insufficient support from the executive team for cybersecurity expenditure and activities, a last resort to obtain backing is to make the board aware of cybersecurity risks. Regulatory momentum in recent years has made board directors more open to discussions about cybersecurity. In particular, the Securities and Exchange Commission in the U.S. has adopted a new rule to enhance and standardize disclosures on cybersecurity risk management across all public companies that are subject to the reporting requirements of the Securities Exchange Act (see https://www.sec.gov/files/rules/final/2023/33-11216.pdf).

Recommendation 3. Leverage Collaboration Opportunities

The completeness and alignment success conditions require OT, IT and cybersecurity personnel to collaborate from the beginning of an OT initiative to develop an integrated cybersecurity solution, and this will likely mean forming cross-functional teams. The benefits of such teams can be far-reaching, as indicated by the IT director of Chemicals Company 1. He said that OT experts in the company's digital transformation team are pivotal in identifying anomalies and assisting in the identification of false positives, thus also reducing the amount of work of the cybersecurity team.

Moreover, having on-the-ground collaboration between different departments can foster a shared understanding of the advantages provided by the cybersecurity solution. Similar to other risk management disciplines, understanding the benefits of cybersecurity requires an accurate assessment of the risks an organization might encounter if the solution was not in place. Though there is currently no established standard in cybersecurity to accurately quantify the benefits of a solution,[28] conducting even basic assessments in collaboration with OT personnel could be advantageous. This is especially relevant as OT professionals often perceive cyber risks as largely disconnected from their day-to-day operations, and, as the Energy Company's OT digital transformation manager pointed out, these collaborative assessments can play a major role in "illustrating the potential impacts of cyber threats on operational reliability."

Furthermore, as digital technologies become ubiquitous in OT environments, creating clearly defined cross-functional teams is increasingly important to prevent inefficient overlaps between units. The demarcation of responsibilities is already shifting significantly, especially considering the increased emphasis on production analytics and system monitoring. As explained by the CIO of Food Processing Company 3, it is better to delineate such teams and their responsibilities as soon as possible, because further technological evolutions (e.g., the progressive transition of OT systems to the cloud) will likely spark increasingly heated discussions about governance and control of the new digital solutions.

28 However, several methodologies are available, both quantitative (e.g., the FAIR model, available at https://www.fairinstitute.org/) and qualitative (e.g., self-assessments based on the National Institute of Standards and Technology Cybersecurity Framework, available at: https://www.nist.gov/cyberframework).

Interdepartmental collaboration can also have positive side effects that might otherwise be overlooked, such as strategic synergies or the realization of benefits not directly related to cybersecurity. These side effects can vary greatly depending on the type of OT initiative, making it challenging to provide precise advice on how to action this recommendation. However, focus group participants identified two scenarios that can help organizations leverage collaboration opportunities. The first is the case of the Oil and Gas Company, which relocated OT servers from factories to centralized data centers. By virtualizing OT servers, the company's IT team was able to create redundancies, which enabled it to manage the load, apply patches and revert to previous states, all without disrupting production processes. The CIO/CDO said:

> *"It takes a lot of money and a lot of time, but it's better. And once the production teams understand this and see the value, they start supporting you. What we have taken over is the full OT infrastructure. All the maintenance and the responsibility of the hardware and the communication. And I think it turned out to be a win-win, because on one side they did not want to focus there [on cybersecurity], and on the other, the company improved in terms of [its] cybersecurity posture."*

In the second case, Food Processing Company 3 leveraged the transparency guaranteed by having all new digital OT systems monitored and under control, as described by the CISO:

> *"Back in 2019, the equipment on the factory floor was maintained directly by the engineering function, but they began to realize they were lacking transparency on precisely what was connected. Consequently, we engaged with them in a security exercise. It was a great business case for them because we utilized the security technology to gain transparency on what exactly was connected. Today, they can access this information live, which they couldn't before. They can see what is happening behind the scenes, what is connected, and use this to optimize the factory and many other operational aspects. So, while we had a slightly rocky start with the deployment, later the engineering function began to spread the word about the value they derived from the solution across the factories, and all of them wanted it immediately."*

Concluding Comments

Industry 4.0 and equivalent initiatives that introduce new digital capabilities to OT environments are vital for industrial companies to stay competitive, responsive and innovative in an increasingly interconnected landscape. But any industrial company will need to ensure that this new OT environment is fully supported by a comprehensive cybersecurity program. Our research offers valuable insights into the organizational success conditions for OT cybersecurity initiatives. In this article, we identify the primary obstacles to achieving these success conditions and provide three recommendations for overcoming them.

The aim of this article is to enhance understanding of how to effectively integrate cybersecurity into OT environments. The need for such integration will only grow as organizations embark on digital transformation journeys in both the IT and OT domains. We conclude by suggesting that future research in both the academic and practitioner realms should further investigate how the success conditions we have identified may vary across different types of OT initiatives and how they relate to and are enabled by broader organizational and cybersecurity capabilities.

Appendix A: Focus Groups, Data Collection and Analysis

Because the field of OT cybersecurity is relatively new, we determined that an exploratory, qualitative research approach would be appropriate for our study, based on focus group-based research.[29] Focus groups offer two significant benefits in terms of data collection: they enable participants to interact broadly on a topic within a limited timeframe, and they provide data that reflects a comprehensive, up-

29 Krueger, R. A. and Casey, M. A. *Focus Groups: A Practical Guide for Applied Research*, 2014, SAGE Publications.

Focus Groups Participants

Role[31]	Company ID
CIO[32]	Manufacturing Company 1
Director, OT Digital Transformation	Manufacturing Company 1
CISO	Manufacturing Company 1
CIO[32]	Manufacturing Company 1
CISO	Manufacturing Company 2
Director, Cybersecurity	Manufacturing Company 2
CISO	Manufacturing Company 3
Director, OT Digital Transformation	Manufacturing Company 4
CISO	Manufacturing Company 4
CIO	Manufacturing Company 4
CISO	Food Processing Company 1
CIO	Food Processing Company 1
Director, Cybersecurity	Food Processing Company 2
CIO	Food Processing Company 2
Director, OT Digital Transformation	Food Processing Company 2
CISO	Food Processing Company 3
CIO	Food Processing Company 3
CISO	Logistics Company
CIO[32]	Logistics Company
CIO[32]	Logistics Company
CTO	Logistics Company
CIO	Chemicals Company 1
Director, IT	Chemicals Company 1
CISO	Chemicals Company 1

to-date perspective of the topic, circumventing a narrow focus on challenges unique to a single firm.[30]

Focus Groups Composition

Data collection was conducted over three focus groups that took place between February 2022 and June 2023. All participants in the focus groups were involved in recurring OT initiatives and cybersecurity. In total, the focus groups included 36 participants from 14 different companies (see table above).

There were 22 participants in the first focus group, representing 10 companies. The second focus group was attended by 12 individuals from 11 different companies. The third and final focus group had 25 participants from nine companies. Overall, 20 participants attended only one focus group, nine attended two, and seven were present at all three sessions. Five companies were

30 Morgan, D. L. *Focus Groups as Qualitative Research*, 1996, SAGE Publications.

Focus Groups Participants (Continuation)

Role	Company ID
Director, Cybersecurity	Chemicals Company 2
CIO	Energy Company
Manager, Strategy and Planning	Energy Company
Director, IT	Energy Company
Manager, OT Cybersecurity	Energy Company
Manager, OT Digital Transformation	Energy Company
Director, Cybersecurity	Oil and Gas Company
CIO and Chief Digital Officer (CDO)	Oil and Gas Company
Director, IT	Oil and Gas Company
CIO	Textile Company
CISO	Textile Company
Director, Cybersecurity	Construction Company

represented at just one focus group session, while the other nine were at all three sessions.

The focus groups were carried out in line with the best practices from the literature. To adhere to these practices, the group size never exceeded 25 participants. Additionally, the fact that several participants became acquainted with each other over multiple focus group sessions may have encouraged more open discussions on a confidential topic like cybersecurity.

We began each focus group session by posing a fixed set of core questions and then expanded to a variable set of specific issues later in each session. Each focus group was facilitated by an individual with over 20 years of experience in digital transformation and cybersecurity who has led several similar focus groups in the past. The facilitator's role contributed to the structured approach of the focus group, ensuring equal participation and steering the conversation away from less critical issues.

Generally, the focus groups proceeded as follows: 1) the facilitator began by introducing and explaining the goals and procedures of the meeting, 2) participants (and new participants in subsequent groups) were asked to introduce themselves and their organizations, 3) participants shared and discussed their opinions based on the initial set of questions, and 4) participants delved into further issues that had not emerged earlier. All the focus groups were conducted in English.

Participants in each group were reasonably homogeneous in terms of general understanding of cybersecurity and OT topics. But they were heterogeneous in terms of their seniority and the attributes of their companies. These attributes included general factors (such as industry sector and workforce size) and topic-specific factors (such as OT maturity level and cybersecurity maturity level). We believe that the mix of homogeneity and heterogeneity among participants helped foster lively discussions.

Data Collection and Analysis

The data gathered through the focus groups was analyzed using a combination of deductive and inductive coding to help explain and interpret the findings within a broader context. The focus group data was collected in approximately 120 pages of transcripts, supplemented by additional

31 To ensure the anonymity of the individuals and companies involved, the description of non-C-level roles has been generalized. Participants labeled as directors are individuals who report to C-level executives, whereas managers report to directors.

32 In these companies, the CIO position changed between focus group sessions.

Conditions for the Success of a Technochange Solution[37]

Success Condition	Condition Description	Potential Obstacles
Completeness (Workable Solution)	The solution should be accompanied by relevant organizational changes to address all the necessary adjustments in organizational processes, structures and systems.	Obstacles that reflect a lack of complementary organizational changes (e.g., new skills training, restructuring of units or roles, reallocation of resources, reconfiguration of business processes).
Alignment/ Implementability (Working Solution)	The solution should align with the organizational processes, culture and incentives, fitting seamlessly within the organizational context.	Obstacles that reflect a misfit between the solution and the ways people work (due to company-specific reasons rather than task-specific ones).
Ability to Capture Benefits (Worked Solution)	The solution should translate into measurable results, thus requiring mechanisms for evaluating its impact on organizational performance and outcomes.	Obstacles that lead to absence or misperception of the expected benefits (financial, reputational, organizational, etc.).

handwritten notes from the second session, for which participants did not agree to a formal recording.

We then analyzed the data using a mixed approach of deductive and inductive coding.[33] Deductively, we mapped our data against the conditions of success for a technochange project identified by Markus,[34] starting with initial concept coding. Inductively, we refined and expanded these categories following an open coding methodology.[35] The data analysis stage concluded in June 2023 after we reached code saturation.[36]

Appendix B: Applying the Technochange Concept to Operational Technology Cybersecurity

Technochange is one of the most recognized frameworks for assessing the organizational change aspect of IT-enabled projects. First proposed by Lynne Markus, she defines technochange as the "strategy of leveraging IT to drive organizational change." Markus argues that the implementation of a technochange strategy—i.e., a technochange project—is distinct from both pure IT and pure organizational change projects in several respects. These include the targeted outcomes, the final solution, the necessary resources and the basic approach. To identify exactly what kinds of projects fall into this category, Markus enumerates a set of characteristics typical of a technochange project. According to Markus, a technochange project:[37]

1. Affects people outside the organization
2. Affects more rather than fewer people and occupational groups
3. Is very expensive, projected to take a long time and has the potential to disrupt organizational performance significantly during startup
4. Is revolutionary, not evolutionary.

In light of these characteristics, various authors[38] have claimed that major IT projects (including digital transformations) are, in fact, a form of technochange projects. This perspective is particularly useful in light of Markus's identification of the success conditions for a technochange project. She argues that successful IT projects require only two major conditions:

33 We used an approach similar to the one proposed in Fischer, H., Wiener, M. and Strahringer, S. "Embarking on the Digital Transformation Journey toward a Data-Driven Organization: Empirical Insights into Transformation Starting Points," 31st *European Conference on Information Systems Research Papers* (298), May 2023.

34 Markus M. L., op. cit., March 2004.

35 See Saldana, J. *The Coding Manual for Qualitative Researchers*, 2021. SAGE Publications.

36 Defined as the point where new qualitative data no longer produces additional or unique codes. For more information, see Hennink, M. M., Kaiser, B. N. and Weber, M. B. "What Influences Saturation? Estimating Sample Sizes in Focus Group Research," *Qualitative Health Research* (29:10), January 2019, pp. 1483-1496.

37 Adapted from Markus M. L., op. cit., March 2004.

38 See, for example, Barthel, P. and Hess, T. "Are Digital Transformation Projects Special?" *Proceedings of the 23rd Pacific Asia Conference on Information Systems*, July 2019.

a functional IT solution (along with its support system) and effective project management that adheres to the planned schedule and budget. In contrast, a technochange project demands three additional success conditions: completeness, alignment/implementability and the ability to capture benefits. Markus contends that the absence of one or more of these conditions leads to non-use or misuse of the solution or to failure in capturing its promised benefits, thereby negating its value proposition. Moreover, Markus points out that each of these success conditions can be undermined by specific "showstoppers," obstacles that can hinder their realization (see table in the previous page).

Building on these conceptual foundations, we believe that the implementation of a cybersecurity strategy, conceived as an integral part of an OT initiative, is equivalent to a technochange project. We argue that for such a project to be successful, it requires a solution that extends beyond the usual IT solution requirements (technical functionality and effective project management) and also encompasses the three success conditions identified by Markus—completeness, alignment/implementability and the ability to capture benefits.

About the Authors

Nico Abbatemarco

Nico Abbatemarco (nico.abbatemarco@sdabocconi.it) is a lecturer in the Leadership, Human Resources and Digital Technologies Department at SDA Bocconi School of Management, Italy. He is also part of the core team of the school's Digital Enterprise Value and Organization (DEVO) Lab, where he studies digital transformation and its impact on organizations. Since 2019, Nico has been part of the team behind the EU and U.S. chapters of the Digital Strategies and Corporate Information Security roundtables, two knowledge-sharing initiatives that address the needs of CIOs and CISOs of large global corporations.

Hans Brechbühl

Hans Brechbühl (hans.brechbuhl@sdabocconi.it) is an associate professor of practice at SDA Bocconi School of Management, Italy, where he leads corporate initiatives on digital transformation, information security and cybersecurity, and their organizational impact. He is the director of the Digital Strategies and the Corporate Information Security Roundtables, programs for large companies in Europe and the Americas. He focuses on the role of CIOs and CISOs in large enterprises and the challenges of cyber/information security in a collaborative, networked environment. Previously, he was the executive director of the Center for Digital Strategies and an adjunct professor at the Tuck School of Business, New Hampshire.

