Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 2280–2290
https://doi.org/10.54941/ahfe1007040

Balancing Agility, Operational Business Requirements and Cybersecurity in a Large Public Organization

Mascha van Dort[1] and Rick van der Kleij[1,2]

[1]Netherlands Organizations of Applied Scientific Research TNO, The Hague, The Netherlands
[2]Avans University of Applied Sciences, Breda, The Netherlands

ABSTRACT

IT departments have shifted towards agile development and self-steering teams, leading to fragmented management of enterprise cybersecurity. This may hinder effective cybersecurity as it requires coordinated efforts and unified decision-making. This study investigates the challenges of agile organizations in enterprise cybersecurity and, more specifically, addressing ransomware threats. To achieve this, we interviewed nine cybersecurity professionals from a large, agile public organization in Europe. From the results of these interviews, we identified 25 challenges that we believe are universal across organizations prioritizing agile teams. To resolve these challenges and ensure optimal cybersecurity practices we propose two novel approaches to organizing enterprise cybersecurity in large-scale agile organizations: boundary spanning and short cycled cyber improvements programs.

Keywords: Enterprise cybersecurity, Large-scale agile, Ransomware, Boundary spanning, Short cycled innovation programs, Cyber resilience

INTRODUCTION

Enterprise cybersecurity is a multifaceted domain that encompasses people, organizational structures, budgets, technologies, processes, and external compliance requirements (Donaldson et al., 2018). It requires coordinated efforts and unified decision-making, especially in large organizations (Abbasi, Petford and Hosseinian-Far, 2021). The increasing frequency and impact of cyberattacks, including ransomware, which affect multiple systems and teams, underscores the need for such coordinated efforts (Allianz Commercial, 2024). Over the years, however, IT departments have evolved significantly, prioritizing agile development and self-steering teams (Crnogaj, Tominc and Rožman, 2022), (Petermann and Zacher, 2021). Agile and self-steering teams share key traits: autonomy, collaborative decision-making, and minimal hierarchical structure (Crnogaj, Tominc and Rožman, 2022; Petermann and Zacher, 2021). The shift to agility with agile development and self-steering teams has transformed organizations from a top-down to a bottom-up approach (Crnogaj, Tominc and Rožman, 2022). In large-scale agile organizations, communication across teams is often self-organized

and, when present, organized around development dependencies (Berntzen, Stray and Moe, 2021). Consequently, management of cybersecurity processes has become more and more fragmented across various agile teams. This fragmentation may hinder coordination and lead to an over-reliance on tools to bridge communication gaps. At the same time, the absence of unified decision-making complicates the enforcement of security controls, such as policies and exception management, the design and implementation of new security processes, security engineering, risk management and mitigation, and overall cybersecurity improvement. The key question of this paper is how to address these challenges of large agile enterprises in managing cybersecurity.

This research uses qualitative data from interviews with nine cybersecurity professionals from different IT-security teams in a large and highly digitalized and agile public organization in Europe. Our objective was to identify challenges to the multifaceted approach of a ransomware threat to organizations that prioritize agile IT development and self-steering teams and to find solutions to these challenges.

We start our paper with a short discussion on the theoretical pitfalls of balancing agility and cybersecurity in large agile organizations. We also discuss the challenges that may result from decentralizing cybersecurity responsibilities. We then describe our study methodology and the sample of cybersecurity professionals we interviewed. Then we present and discuss challenges experienced by our respondents when trying to manage cybersecurity. We also show how these challenges reverberate across theories of systemic thinking, resilience, social identity theory and practices of communication and program management. We then propose two novel approaches to organizing cybersecurity in large-scale agile organizations, resolving tensions in enterprise cybersecurity that follow from the challenges identified, ensuring the optimal performance of enterprise cybersecurity functions within agile frameworks.

BACKGROUND

Over the past five years, there has been a notable expansion in large-scale agile practices. This expansion has resulted in the proliferation of agile teams within enterprises, fostering decentralized structures and some form of self-managing teamwork, also in IT departments (Crnogaj, Tominc and Rožman, 2022). The trend towards agility and decentralized teams is driven by the need for responsiveness and adaptability in a rapidly changing business environment (Petermann and Zacher, 2021).

Notwithstanding the current trend towards agility and decentralized teams, substantial literature advises against the decentralization of IT security responsibilities to individual teams—citing risks such as diluted responsibility, weakened accountability of security capabilities, and compromised governance, which collectively heighten the risk of security breaches (Abbasi, Petford and Hosseinian-Far, 2021). This cautionary stance advised in literature appears to conflict with the current trend in IT departments towards agile development and decentralized, self-steering teams.

Balancing these two aspects—agility and cyber security—requires careful consideration and often innovative approaches to ensure that security

measures are robust without stifling the benefits of agile practices (Nägele, Watzelt and Matthes, 2022). The caution against decentralizing IT security responsibilities is primarily driven by concerns regarding inadequate joint decision-making and communication across agile teams and departments within organization. Effective communication and decision-making across agile teams could overcome those concerns. While the methodologies employed by agile development teams are extensively documented, practical frameworks for effective communication and decision-making across these teams remain underdeveloped. Scientific literature does address frameworks for effective communication to some extent stressing the importance of coordination strategies. (Berntzen, Stray and Moe, 2021).

METHOD

Nine cybersecurity professionals from a large, agile organization participated in our study. This public organization employs over 25,000 people. The IT department, responsible for all IT and IT security, is one of the largest in Europe with over 3,000 employees and is divided into several sections. From this IT department, a total of nine professionals were selected, at least one from each of these sections based on their expertise in IT security and ransomware to participate in our research. Interviews were conducted with all nine employees. The procedure was as follows. After an introductory round, we discussed challenges respondents experience in managing the risk of ransomware attacks. Ransomware attacks was chosen as the main topic in these discussions because several studies show that ransomware is the biggest threat for enterprises around the world, requires coordinated efforts to resolve, and is hard to defend against (Mandiant, 2024). To structure the interviews we used the NIST CSF 2.0 framework (Pascoe, 2023). The NIST CSF 2.0 framework is implemented throughout the organization and all respondents were familiar with it. For each of the 6 phases in the framework, identify, protect, detect, respond, recover, and govern, we asked the respondents for challenges they encounter in their work. The interviews took approximately 1 hour each.

RESULTS

The interviews revealed several challenges for each of the different NIST 2.0 phases in enterprise cybersecurity which are collected in table 1. For a complete overview of the interview results see table 2 in the Annex of the paper. Further analysis identified two fundamental sets of challenges that we believe are quite common in large, agile organizations today. The first collection of challenges is evidence of an internal tension of balancing agility and cyber security in (de)centralized cyber security. Our respondents stated that while cybersecurity improvements were easily identified, their implementation was slow, and risk management across business units, IT divisions within the IT organization, and underlying self-steering teams within these divisions was inadequate. Despite unanimous agreement on the benefits of self-steering teams and agile practices, there was a clearly expressed need for better collaboration and decision making across teams, IT divisions and operational business units regarding cyber security. Further,

when considering the multifaceted domain of enterprise cybersecurity: people, process, and technology (Assibi, 2023), efficient processes for cross organizational risk management and management of security controls throughout the organization were found to be lacking (Donaldson et al., 2018).

Table 1: Challenges and tensions.

Challenges	Tension
Lack of Cross-Organizational Risk Management Unclear guidelines Poorly Defined Roles Inconsistent Security Practices Ineffective Security Governance Communication and Collaboration Issues Departmental Silos Fragmented Security Responsibilities	Balancing agility and cyber security in (de)centralized cyber security decision making about security controls and risk management
Lack of Security Prioritization Resource Constraints Unclear Guidelines Unclear Decision-Making Authority Communication and Collaboration Issues Uncoordinated Security Efforts Resistance to Change Slow Implementation of Security Measures Delayed Security Projects	Balancing operational business requirements and cybersecurity improvements

Examples of the challenges in balancing agility and cybersecurity in (de)centralized decision-making about security controls and risk management included: "The CTO department needs to take more initiative, just like this meeting. Because there is no lead, you see departments picking things up themselves" (Ineffective Security Governance); "It's unclear which departments or individuals should handle certain policy questions" (Unclear Guidelines); "It is difficult to determine who should take which step"; and "Each department is working in isolation, but organization-wide checks are missing" (Departmental Silos). The effects of these challenges were also noted, such as: "There is little risk alignment across the entire chain," and "Risk acceptances are going wrong, especially on projects that 'just need to move quickly'" (Lack of Risk Management). The organization was struggling with typical obstacles blocking horizontal communication between organizational structures such as departmental silos (Scott and Gong, 2021) and consequent fragmented security responsibilities, unclear guidelines (Riege, 2005), poorly defined roles (Scott and Gong, 2021), leading to inconsistent security practices (Tett, 2016), while at the same time leaving responsibility for cyber security controls and risk management– which needs horizontal communication and decision making- in the teams.

A second collection of challenges entails around an internal tension of balancing operational business requirements and cybersecurity improvements. Hence, improvement projects often failed, according to our respondents, due to a lack of essential elements such as the appropriate team, sponsor, time, and priority (Iske, 2018), (Govindarajan and Trimble, 2010). This failure was frequently attributed to a lack of organizational transparency and the inherent complexity of the organization. We defined this collection as a tension of balancing operational business requirements and cybersecurity improvements.

Examples of balancing operational business requirements and cybersecurity improvements included statements such as: "What is holding you back? Money, time. Even if it serves security, security is at the bottom" (Lack of Security Prioritization); "An administrator prefers no changes" (Resistance to Change); "Every team wants us, but that is not feasible" (Resource Constraints); and "Speed is lacking, and due to the size of the organization, it is currently not possible to accelerate this" (Lack of Time for Operational Project Team Members). This impacted the organization in the following ways: "Migration is still taking place; it will take another four years to reach a complete plan," and "Innovation takes a long time" (Slow Implementation of Security Measures). Further analysis revealed unclear project sign on and sign off (Riege, 2005), (Iske, 2018), lack of time for improvement projects by operational members (Govindarajan and Trimble, 2010), leading to analysis paralysis (Iske, 2018) and slow implementation of improvement measures and delayed innovation projects (Tett, 2016), (Govindarajan and Trimble, 2010).

Upon analyzing the categories, it was found that "governance and management challenges" were the most prevalent. Followed by "communication and collaboration challenges." "Resource and prioritization challenges" came next. "Cultural challenges" were mentioned only relatively few. This was particularly striking, as management emphasized, in the talks we had with them prior to the interviews, the need for cultural change.

When reflecting on all the challenges reported, widespread neutralization techniques, i.e., types of rationalizations, were identified (Siponen, Puhakainen and Vance, 2020), that endanger the optimal functioning of enterprise cybersecurity within agile frameworks, such as: "Someone else should take responsibility for this, but it's not being addressed (denial of responsibility')." Hence, the person rationalizes that the action in question is beyond his or her control (Piquero et al., 2005). Also, some decision-making biases were observed. For instance, there was an over emphasis on analysis leading up to a failure of execution: "To have a plan, we first need to know exactly how this service runs across the platforms (analysis paralysis)." Analysis paralysis is the inability to decide due to overthinking. Decentralized teams were struggling due to a lack of guidelines and structure (processes) for collaboration and decision-making in the large-scale agile organization, despite the quality of people and technology. Respondents themselves noted: "Delegating responsibility to teams is good, but we need guidelines for collaboration across teams."

DISCUSSION

Interviews revealed cybersecurity challenges in a large-scale public agile organization, rooted in two internal tensions: balancing agility with cybersecurity, and aligning operational business needs with security demands. These tensions can be attributed not to the external pressures of a fast-changing risk landscape, but to the contested rationalities of operational business requirements and cybersecurity (Dupont et al., 2023).

When we look more closely at the tension of balancing agility and cybersecurity, we see some resemblance with mechanistic thinking. In mechanistic thinking, it is assumed that an organization consists of the sum of its parts that communicate and collaborate through 'bridges'. Peter Senge, known for his work "The Fifth Discipline (Senge, 1997)," describes mechanistic thinking as a limited way of thinking that often causes problems in organizations. Mechanistic thinking assumes an organization is merely the sum of its parts—departments connected by functional 'bridges'. According to Senge, this leads to the reduction of complex problems to isolated elements, without sufficient attention to interrelationships and interactions.

Senge (Senge, 2006) argues that mechanistic thinking is at the core of many organizational problems because it simplifies dynamic and complex processes in organizations into discrete tasks and functions. Instead of seeing the whole, organizations often focus on fragments, missing underlying patterns and interdependencies. This mechanistic view fosters silo thinking, where departments operate in isolation, hindering collaboration and organizational awareness. Silo thinking is a specific form of mechanistic thinking that focuses on the organization of people and teams within an organization. This can lead to cybersecurity being seen as purely a technical responsibility of the own team, without the involvement of HR, legal, and other departments essential for sustainable cybersecurity. As a result, there is often a lack of insight into the broader context and the impact of one's work on other departments. This can lead to inefficiency and conflicts between departments and a fragmented approach to security measures.

To resolve this tension, a more systemic approach is required. An approach that recognizes that security cannot be reduced to merely the sum of all technical measures a company takes, but is the result of constant interactions between all elements necessary to deliver essential functions and services (Dupont et al., 2023), (Dunn Cavelty, Eriksen and Scharte, 2023) and (Dupont, 2019). A systemic or systems thinking approach to cybersecurity posits that an organization is a set of complex elements that adapt to, respond to, and influence each other.

Hence, we dare to say that systems thinking is essential for enterprise cybersecurity. Cyber threats are complex, dynamic, and often unpredictable phenomena that cannot be solved in isolation. A purely mechanistic approach would focus solely on strengthening technical defenses such as firewalls and antivirus software, but this is usually not enough to make an organization truly resilient against cyber threats. Systems thinking offers a broader, integrated approach by analyzing the interactions between people, technology, and the organization as a whole and promoting collaboration

between organizational units that play a role in cybersecurity. In utilizing a more systemic approach to cybersecurity, organizations could employ so called boundary spanners. Boundary spanners enhance communication and decision-making by linking teams across the organization (Williams, 2012). The role of the boundary spanner is primarily to communicate with the organization (typically the executive suite) and to direct the overall objectives of the larger organization to the individual component teams. Hence, boundary spanners facilitate interactions among component teams, ensure that organizational resources are available when needed, and act as a tiebreaker for the component teams when necessary. The boundary spanner takes on the leadership role in a fragmented agile cybersecurity organization, performing unified decision-making and inter-team coordination activities that have been deemed important in the enterprise cybersecurity strategy. Boundary spanners could add vital functionality in fragmented agile organizations, performing unified decision-making and inter-team coordination activities, which are important in cybersecurity strategies.

The second tension—balancing business needs with cybersecurity improvements—mainly stems from out-group bias and differing rhythms between operations and innovation.

In cybersecurity, responsibilities are divided among different groups: the Chief Technology Officer (CTO) office, which is responsible for policy making; the operational IT departments and sections, which manage risks and ensure compliance with policies; and the Security Operations Center (SOC), which monitors, detects, and responds to security incidents. This distinction in responsible teams can lead to differences in perspectives and priorities, often resulting in tension between agile and self-steering teams.

Social Identity Theory (Tajfel, 1979) suggests employees may favor group norms over organizational cybersecurity policies, hindering improvements. This can lead to inconsistent adherence to security protocols if the group norms do not emphasize cybersecurity (reported as leading to inconsistent security practices). There may be resistance to adopting cybersecurity measures or best practices developed by other teams or departments. This "Not Invented Here" syndrome can hinder the implementation of effective security solutions (out-group bias). Social Identity Theory suggests that people are more likely to collaborate and communicate effectively within their in-groups. Encouraging intra and cross-departmental collaboration and creating a unified cybersecurity culture can help bridge gaps between different teams within the organization.

Govindarajan and Trimble argue in their work The Other Side of Innovation (Dupont et al., 2023), that the different roles of operational and dedicated staff can significantly affect innovation and improvement. While operational expertise is essential for the realization of innovations, operational departments have a different operating rhythm, power balance, and depth of relationships compared to what is needed for executing innovations. Therefore, to organize cyber improvements projects effectively, it is important to have both members from operational departments and dedicated innovation staff, often coming from the CTO department.

The continuous need for improvements in cybersecurity throughout the organization brings about challenges typical of both the organization of innovation execution and the tension between innovation and operational rhythms. Not only does it involve adopting cybersecurity measures or best practices developed by external project teams, but the progression of improvement projects might also be hindered by different priorities and operational rhythms.

To overcome challenges and facilitate improvements, we propose a program approach for enterprise cybersecurity projects. A program coordinates related projects to achieve strategic cybersecurity goals (Trzeciak, Kopec and Kwilinski, 2022). Programs manage interdependencies, facilitate decision making, allocate resources, and align projects with organizational strategy, ensuring effective management and progress.

To ensure innovation success, overall cybersecurity effectiveness, and overcome out-group Bias, we suggest a short-cycled approach with clear goals for each phase and the use of supporting canvases. APG applied this method in 2018, organizing innovation into four agile phases: explore, experiment, pilot, and scale out (Beukers et al., 2018). Each phase has specific objectives, and a standardized way of working ensures maximum innovation success with minimal effort.

The Partnership for Cyber Security Innovation (PCSI) adapted this method for collaborations between Dutch financial institutions on cybersecurity innovation (Wolthuis, 2022). Phases were executed within a four-month cycle, allowing go/no-go meetings for all projects to be held on the same day with a joint steering committee, attended by all participants. It was found that this setup enabled the spread of innovative insights across the ecosystem. A steering committee ensured that bank personnel had the capacity to participate, while researchers facilitated the program. Presentations were conducted by bank personnel to promote inclusivity and counteract out-group bias.

Integrating program management with a short-cycled approach helps counter out-group bias, align cybersecurity with strategy, and bridge the gap between operations and innovation. This approach also guarantees timely progress of improvement projects, balancing operational business needs with cyber-resilience enhancements. An additional benefit of this program is that the structured communication of cyber improvement results every four months among all program participants leads to enhancement of shared cybersecurity awareness on both operational and managerial level, which was one of the most frequently reported challenges in the current research.

PRACTICAL IMPLICATIONS

The practical implications of this research are extensive. We anticipate that the need for responsiveness and adaptability in a rapidly evolving business environment will further drive the adoption of agile work practices within enterprises, characterized by decentralized structures and self-managing teams. This shift influences the approach to cybersecurity governance in large-scale agile organizations. Instead of relying on centralized governance,

new governance models for risk management, cyber controls, and cyber improvement projects should be developed to align with decentralized agile governance. This article proposes two new structures to ensure enterprise cybersecurity in large-scale agile organizations: Boundary Spanning and Short-Cycled Cyber Improvement Programs.

ANNEX

Table 2: Main challenges prioritized by occurrence including categories.

	Challenges	Occur-Rence	Category
1	Lack of Shared Cyber Security Awareness	High	Communication and Collaboration Problems
2	Lack of Cross Organizational Risk Management	High	Governance and Management Problems
3	Lack of Security Prioritization	Medium	Resource and Prioritization Problems
4	Resource Constraints	Medium	Resource and Prioritization Problems
5	Unclear Guidelines	Medium	Communication and Collaboration Problems
6	Communication and Collaboration Issues	Medium	Communication and Collaboration Problems
7	Inconsistent Security Practices	Medium	Governance and Management Problems
8	Ineffective Security Governance	Medium	Governance and Management Problems
9	Poorly Defined Roles	Medium	Governance and Management Problems
10	Resistance to Change	Medium	Cultural Problems
11	Slow Implementation of Security Measures	Medium	Governance and Management Problems
12	Unclear Decision-Making Authority	Medium	Communication and Collaboration Problems
13	Uncoordinated Security Efforts	Medium	Communication and Collaboration Problems
14	Analysis Paralysis	Low	Governance and Management Problems
15	Autonomy vs. Centralization	Low	Governance and Management Problems
16	Cultural Issues	Low	Cultural Problems
17	Departmental Silos	Low	Governance and Management Problems
18	Fragmented Security Responsibilities	Low	Governance and Management Problems
19	Lack of Comprehensive Security Vision	Low	Governance and Management Problems
20	Lack of Integrated Security Approach	Low	Governance and Management Problems

Continued

Table 2: Continued

	Challenges	Occur-Rence	Category
21	Lack of Time for Operational Project Team Members	Low	Resource and Prioritization Problems
22	Technical and Organizational Problems	Low	Governance and Management Problems
23	Delayed Security Projects	Low	Governance and Management Problems
24	Fear of Making Mistakes	Low	Cultural Problems
25	Lack of Leadership Support	Low	Governance and Management Problems

REFERENCES

Abbasi, K., Petford, N. and Hosseinian-Far, A. (2021) 'Centralised IT Structure and Cyber Risk Management,' in Cybersecurity, Privacy and Freedom Protection in the Connected World. Cham: Springer International Publishing, pp. 357–366.

Allianz Commercial (2024) Allianz risk barometer. Münich: Allianz Commercial.

Assibi, A. T. (2023) 'Literature Review on Building Cyber Resilience Capabilities to Counter Future Cyber Threats: The Role of Enterprise Risk Management (ERM) and Business Continuity (BC),' Open Access Library Journal, 10(4), pp. 1–15.

Berntzen, M., Stray, V. and Moe, N. B. (2021) 'Coordination strategies: managing inter-team coordination challenges in large-scale agile,' in International Conference on Agile Software Development. Cham: Springer International Publishing, pp. 140–156.

Beukers, J. et al. (2018) Innovation Manual. Heerlen: GroeiFabriek.

Crnogaj, K., Tominc, P. and Rožman, M. (2022) 'A conceptual model of developing an agile work environment,' Sustainability, 14(22), p. 14807.

Donaldson, S. E., Siegel, S. G., Williams, C. K. and Aslam, A. (2018) Enterprise cybersecurity study guide: How to build a successful cyberdefense program against advanced threats. New York: Apress.

Dunn Cavelty, M., Eriksen, C. and Scharte, B. (2023) 'Making cyber security more resilient: Adding social considerations to technological fixes,' Journal of Risk Research, 26(7), pp. 801–814.

Dupont, B. (2019) 'The cyber-resilience of financial institutions: significance and applicability,' Journal of Cybersecurity, 5(1), p. tyz013.

Dupont, B., Shearing, C., Bernier, M. and Leukfeldt, R. (2023) 'The tensions of cyber-resilience: From sensemaking to practice,' Computers & Security, 132, p. 103372.

Govindarajan, V. and Trimble, C. (2010) The other side of innovation: Solving the execution challenge. Boston: Harvard Business Press, pp. 77–87.

Iske, P. L. (2018) Instituut voor briljante mislukkingen: Maak ruimte om te experimenteren, innoveren en leren. Amsterdam: Business Contact, pp. 122–123.

Mandiant (2024) M-Trends 2024 Special Report. Virginia: Mandiant.

Nägele, S., Watzelt, J.-P. and Matthes, F. (2022) 'Investigating the current state of security in large-scale agile development,' in International Conference on Agile Software Development. Cham: Springer International Publishing, pp. 203–219.

Pascoe, C. E. (2023) 'Public Draft: The NIST Cybersecurity Framework 2.0.'

Petermann, M. K. H. and Zacher, H. (2021) 'Development of a behavioral taxonomy of agility in the workplace,' International Journal of Managing Projects in Business, 14(6), pp. 1383–1405.

Riege, A. (2005) 'Three-dozen knowledge-sharing barriers managers must consider,' Journal of Knowledge Management, 9(3), pp. 18–35.
Scott, I. and Gong, T. (2021) 'Coordinating government silos: challenges and opportunities,' Global Public Policy and Governance, 1(1), pp. 20–38.
Senge, P. (2006) 'Systems citizenship,' in The Leader of the Future 2: Visions, Strategies, and Practices for the New Era, pp. 31–46.
Senge, P. M. (1997) 'The fifth discipline,' Measuring Business Excellence, 1(3), pp. 46–51.
Siponen, M., Puhakainen, P. and Vance, A. (2020) 'Can individuals' neutralization techniques be overcome? A field experiment on password policy,' Computers & Security, 88, p. 101617.
Tajfel, H. (1979) 'An integrative theory of intergroup conflict,' in The Social Psychology of Intergroup Relations. Monterey, CA: Brooks/Cole.
Tett, G. (2016) The silo effect: The peril of expertise and the promise of breaking down barriers. New York: Simon and Schuster, pp. 51–106.
Trzeciak, M., Kopec, T. P. and Kwilinski, A. (2022) 'Constructs of project programme management supporting open innovation at the strategic level of the organisation,' Journal of Open Innovation: Technology, Market, and Complexity, 8(1), p. 58.
Williams, P. (2012) 'We are all boundary spanners now?,' in Collaboration in Public Policy and Practice. Bristol: Policy Press, pp. 95–118.
Wolthuis, R. (2022) 'Orchestrating Innovation for Cyber Security Partnership for Cyber Security Innovation-PCSI,' Presentatie op TNO Marktdag Cybersecurity 16–6-2022.