ISSN: 2687-8097
DOI: 10.33552/SJRR.2019.02.000536
Scientific Journal of Research and Reviews
Iris Publishers

Review Article

Cybersecurity Readiness: An Empirical Study of Effective Cybersecurity Practices for Industrial Control Systems

Anderson Domingues Pereira da Silva and Yuri Bobbert*

Antwerp Management School, Belgium

***Corresponding author:** Yuri Bobbert, Antwerp Management School, Belgium.

Received Date: December 11, 2019

Published Date: December 18, 2019

Abstract

Industrial Control Systems (ICS) were primarily designed to operate air-gapped; however, the pressure for cost reduction and integration with business systems demanded the adoption of open systems architecture and ended up exposing ICS to threats which until then had been restricted only to the Information Technology (IT) systems. Although Cybersecurity Standards for Industrial Control Systems have been in place since the 1990s, providing the foundational knowledge required to Secure Industrial Control Systems; implementation failures and media disclosures revealed that organizations are not yet prepared to deploy Cybersecurity Controls effectively. This research has employed Design Science and interaction with experts on a qualitative manner exploring new insights and allowing to identify the main barriers for deploying and assessing industrial control systems. The results of this research include a list of Practices for effective deployment of Cybersecurity controls; list of Critical Success Factors for assessing ICS; and a list of most effective ways to report Cybersecurity risks to the board. This research counted with the participation of 200 practitioners and experts from Europe, Asia, Americas and Oceania.

Keywords: Index Terms Industrial Control Systems; Cybersecurity; Design Science Research; Group Support System research

Introduction

Industrial Control systems, (also referred as Supervisory Control and Data Acquisition, SCADA) are often deployed in manufacturing processes and in controlling Critical Infrastructure (energy, water, oil and telecommunications). Designed for safety and reliability and capable of recovering from process faults and failures, these systems have been widely used for monitoring and controlling physical processes. The ICS transformation from proprietary (isolated systems) to open architectures and standard technologies has exposed ICS to significant new threats. Although cybersecurity standards and guidelines have being developed by governments and standards associations, companies and institutions are not deploying Cybersecurity Controls on ICS effectively, leaving business and critical infrastructure at risk, with possible impact on the economy and human lives.

Problem Statement

Although it seems the topic has gained in importance, the number of incidents involving SCADA systems is still increasing. According to Auffret et al. [1] "Cybersecurity for Industrial Control Systems has not been addressed adequately both in terms of technology but, most importantly, in terms of organizational leadership and policy," Nicholson et al. [2] on his paper "Cybersecurity in the light of a Cyber Warfare, had also highlighted that "Whilst contemporary research has identified the need for protecting SCADA systems, these information are disparate and do not provide a coherent view of the threats and the risks resulting from the tendency to integrate these once isolated systems into corporate networks that are prone to cyberattacks."

According to the Information Systems Audit and Control Association (ISACA), a world-renowned practitioner-oriented body with members worldwide - ISACA [3], "while it is important to have corrective controls in place to respond to an exploited vulnerability, it is more important to ensure preventive controls are operating effectively and efficiently to mitigate the probability of an attack." Earlier in 2014, ISACA performed a survey involving 32 Dutch organizations in an effort to identify the main reasons why companies are not succeeding in deploying Cybersecurity Controls, Franken [4], the survey results revealed that most of

the organizations have "difficulties in performing Cybersecurity Assessments and extensive tests."

Based on the work of Auffret [1], Nicholson [2] and Franken [4], we have evidences that more attention has been drawn to the topic of ICS Cybersecurity; however: "Companies and Institutions are not deploying Cybersecurity Controls on ICS / SCADA) effectively, on a technical level and also at the organizational level, leaving business and critical infrastructure at risk, with possible impact on the economy and human lives."

Research Objective

Considering the problem described, the main research objective is "Examine why companies and institutions are failing to deploy Cybersecurity Controls in Industrial Control Systems Environments and to propose practices that could enable them to effectively address Cybersecurity Risks in Industrial Control Systems Environments."

The aim is to provide details on planning, assessing and reporting Cybersecurity Risks. To achieve this goal the following sub- questions must be answered:

RQ_1: What are the main challenges in deploying Security Controls on ICS/SCADA systems and what are their root causes according to ICS Practitioners and Security Officers?

RQ_2: What are the Critical Success Factors (CSF) in deploying a Cyber Assurance (An assurance cycle which ensures that cyber risks receive targeted levels of audit attention) model for SCADA/ ICS and which CSFs are relevant and should be added to the existing Body of Knowledge according to these ICS Practitioners?

RQ_3: What are the most effective ways to report ICS/SCADA Cybersecurity Risks to the Board and what are the main topics to be reported according to Board members?

Research Methodology

To accomplish that, this research has used Design Science Research (DSR) methodology, DSR places itself as a method connecting the contextual environment (research problem) and the available knowledge at the time of the research; It enables to examine, enrich and validate ICS cybersecurity practices and enhance the current ICS Cybersecurity audit practices/frameworks or spin off new ones. By applying DSR the continuous alignment between rigor and relevance is assured. Figure 1, depicts the framing of this research according to Design Science framework, the literature research (knowledge base) will assist on achieving the Rigor required for this scientific research while "Design science research is comprise of activities related to building and evaluating artefacts designed to meet the identified business needs", (validation of the artefacts by practitioners), "the Relevance Cycle bridges the contextual environment of the research project with the design science activities", (literature review and interview with specialists), "The rigor cycle connects the design science activities with the knowledge base of scientific foundations, experience and expertise that informs the research project", validation by the practitioners and business leaders.

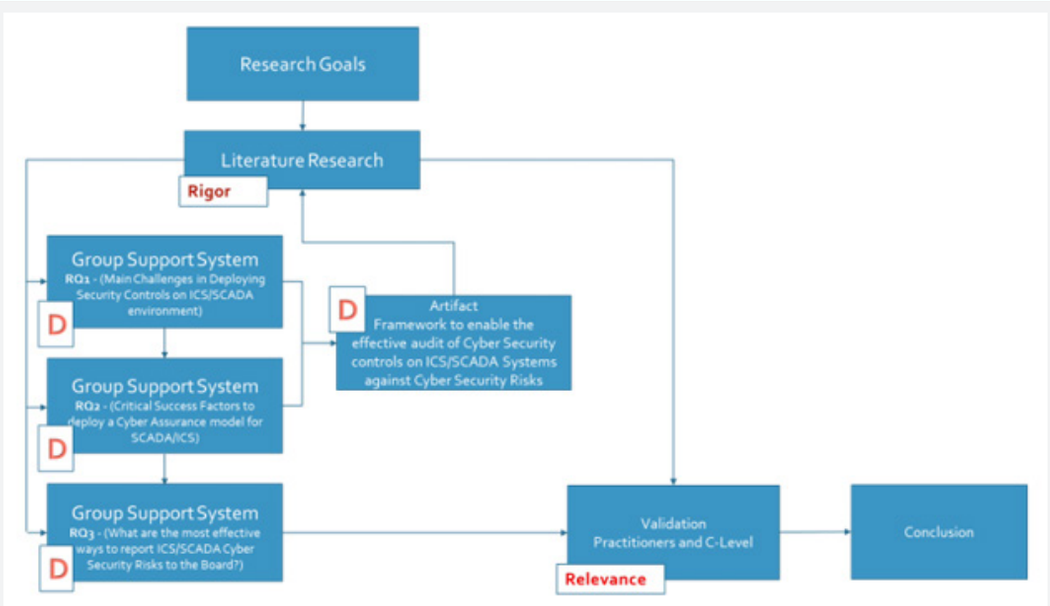


Figure 1: Framing of this research according to DSR.

Bobbert examines DSR as a research approach for the Improvement of Information Security and uses DSR to utilize existing knowledge and frameworks (e.g. NIST and ISF) and to validate and enrich this via the input of the relevance cycle (practical environment), Bobbert [5]. To ensure all the data captured remained reliable and repeatable allowing a further extension of this research work, the GSS (Group Support System) tool was used in documenting every step ensuring repeatability; all activities were time bounded. A knowledge base was built based on literature reviews and the inputs from two GSS Sessions, with 180 participants, ICS Practitioners, ICS Experts and Information Security Practitioners and Executives from several industries, this

practice provided the rigor required to develop the artefacts, that were further analysed and had its relevance validated by means of an online survey performed with 16 participants, mainly ICS Practitioners and Information Security Professionals; "C-Level" executives with participation on executive boards were also consulted on how Cybersecurity risks should be reported to the board (Figure 1).

Research Results

Literature review

The literature review performed during the first six months provided the foundation for the identification of the current challenges organizations are facing in deploying Cybersecurity on Industrial Control Systems, through deductive reasoning, it was obvious, the next step on the research should be the investigation of which factors were negatively influencing the deployment of these controls including pitfalls or roadblocks companies were facing, that has triggered the first exploratory research which was conducted with Information Security specialists and Practitioners from the Industrial Control Systems field, the results of this session combined with further literature review served to elucidate the problems.

The Design Science methodology requires the validation of the produced artefacts by professionals or subject matter experts, the validation of each artefact and its sub-products will be performed on this chapter, the outcome of this research is the delivery of three artefacts.

Artefact 1: A list of critical success factors to deploy an effective Cyber Assurance (a statement, assertion, intended to inspire confidence or give encouragement).

Artefact 2: A list of Practices to enable companies and institutions to effectively implement Cybersecurity controls on ICS.

Artefact 3: Results of a combined research with Practitioners and C-Level executives on how to effectively report ICS/SCADA Cybersecurity risks to the Board.

Main Challenges when deploying Cybersecurity Controls in ICS/SCADA

When asked about the main barriers to deploying Cybersecurity Controls in Industrial Control Systems, the same topics were listed and scored with the same ranking by both groups. A lack of Awareness and Prioritization by the organizations was listed as the main barriers, followed by a poor understanding of ICS Security. The brainstorming session with Practitioners and Information Security Specialists on the main reason for the failure in deploying Cybersecurity Controls on ICS/SCADA re-affirmed the need for more awareness at the corporate level of the topic and the need to build the knowledge necessary to deploy Cybersecurity Controls. Moreover, the inputs from the brainstorming session also helped to identify some of the root reasons why ICS Cybersecurity deployments are failing, such as for instance the lack of structures (roles) and the lack of accountability for the processes described in Table 1.

Table 1: Main reasons for failure in deploying Cybersecurity Controls on ICS (Information Security Professionals and ICS Practitioners).

1	Lack of ownership
2	No clear responsibilities
3	Lack of awareness on the risks
4	No correct role definition for this role
5	Ownership not clear
6	Responsibility matrix not correctly defined
7	Unclear responsibilities
8	Knowledge level / training / expertise / awareness
9	Failure to understand unique manufacturing needs
10	Lack of a big incident in the company

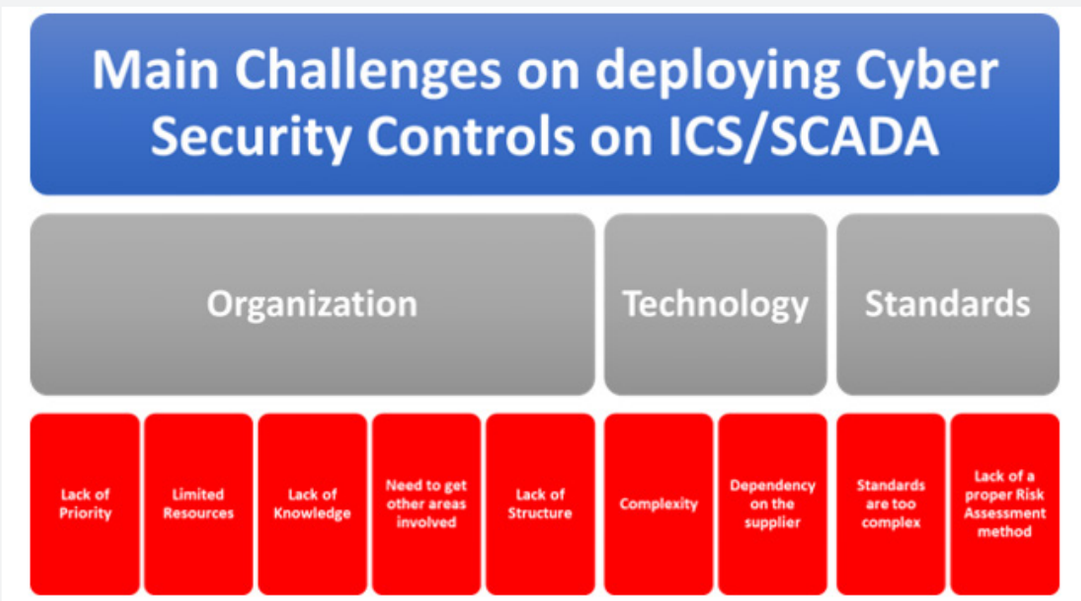


Figure 2: Research Question 1 - Main challenges for deploying Cybersecurity Controls on ICS and SCADA.

Based on the inputs from the analysis of the collected data through two sessions the following the challenges and respective root causes were identified- R-Q_1 (Figure 2).

Organizational Level

Lack of Priority, Limited Resources and a Lack of Structure: Can be directly related to actions or tasks which were identified yet however, are not receiving the necessary importance to be accomplished; setting priorities and allocating resources are typical management activities required to ensure company resources are effectively deployed to achieve business goals. In this case the deployment of Cybersecurity Controls may not be following a consistent approach throughout the organization. , According to the CNPI [6] paper - Security for Industrial Control Systems, "An effective governance framework sets out clear roles and responsibilities, an up-to-date strategy for managing ICS security risk, and provides assurance that the supporting policies and standards are being followed". Harrell [7], in his article for the CSO Online, has said, "Effective cyber risk governance also depends on building trust among the various functions, which will drive behaviour within the organization,," In his analysis of the Organization's Metasystems using Viable System Models, Alqirem [8], he refers to the company senior management (System 3) as the organism responsible for the everyday control of the operations (System 1), and the interaction between the operational units.

Lack of Knowledge: It can be referred to either as a lack of knowledge to perform a certain activity or a lack of awareness around a certain topic. In both cases, the priority set by management should also come together with directions which will need to be communicated followed by action plans that may include training or knowledge acquisition, as depicted by von Solms [9].

Technology Level

Complexity: In the context of Cybersecurity controls for ICS/SCADA – refers to the combination of AICS components and IT components on its intrinsic complexity, when referring to the deployment Cybersecurity controls. "Identifying a reasonably effective set of security controls can be a very complicated and resource-intensive process, which requires special resources and expertise most companies do not possess," Shuchih [10]. As Cybersecurity is still a new domain with very few practitioners, partnership with the information security area and vendor should be the best alternative.

Dependency on the Supplier: Considering ICS/SCADA suppliers are entirely responsible for Hardware, software and deployment of the AICS solutions, it is natural that the dependency is high, "to ensure the secure, reliable and safe operation of information and communications and operational technology systems that are integral to critical infrastructures, organizations must effectively manage risk factors that arise in supply chains for cyber-based products and services. To this end, the Objectives of stakeholders must be clearly understood, and the associated requirements defined precisely and prioritized," Windelberg [11].

Standards

Standards are too complex: Reviewing the responses of the sessions in Rotterdam and The Hague from both groups indicates that ICS/SCADA/DCS operators have overseen deploying cybersecurity controls for Industrial control systems. ICS/SCADA/DCS system operators are the most knowledgeable on a plant or facility in terms of the system safety and reliability requirements; however, they may not be skilled enough on other disciplines currently referred on the existent standards such as Network security, Information Security and Cybersecurity. Therefore, as highlighted by ENISA [12] on its paper "Protecting Industrial Control Systems-Recommendations for Europe and Member states," it's fundamental to provide full guidance to on-field staff regarding a proper understanding of information security and Cybersecurity challenges. One question that remains unanswered in this research is whether the complexity resides in the structure and application of the standard or on the standard content itself. The first should be relevant only to one's responsible for coordinating the implementation of the standard while the second refers to executing the controls, one way or another, knowledge is a capability that must be developed or acquired for ICS Security.

Lack of a proper risk assessment method: ICS/SCADA Systems can be considered complex systems given its cyber physical connections and exchange of data with traditional IT Systems, the horizon of possible threats and vulnerabilities in such a complex environment requires a more comprehensive risk assessment method, although frequently referred to standards, no advice is given on specific Risk assessment methodologies for ICS/SCADA. In order to have a better understanding of the current status of Risk assessment methods specific for ICS/SCADA environment, we came across the paper from Cherdantseva [13] called "A review of Cybersecurity risk assessments methods for SCADA systems," the authors reviewed 24 papers each representing a different Risk Assessment methodology, and although none of the risk assessment methods demonstrated to be ideal, their analysis of the requirements may serve as an input for what should be an ideal method, "Cybersecurity risk assessment methods for SCADA systems may be improved in terms of

i. Addressing the context establishment stage of the risk management process,
ii. Overcoming attack- or failure orientation,
iii. Accounting for the human factor,
iv. The capturing and formalization of expert opinion,
v. The improvement of the reliability of probabilistic data,
vi. Evaluation and validation, and
vii. Tool support, (ibid).

Critical success factors in deploying cybersecurity assurance model for ICS/SCADA

During the session with Information Security Officers and ICS Specialists, participants were asked to rate their current ICS/

SCADA Cybersecurity Risk audit/assessment method on a scale from one 1- Not Effective to 5- Highly effective. As show on Figure 3, 50% of the respondents have score their current audit/assessment method as ineffective or poorly effective while only 12% have score their methods as effective or highly effective. When asked about their main challenges when auditing/assessing heterogeneous ICS/SCADA implementations, according to the 46% of the participants, the challenges reside on the complexity on the existing standards / documentation and the lack of priority at the organization, Figure 4.

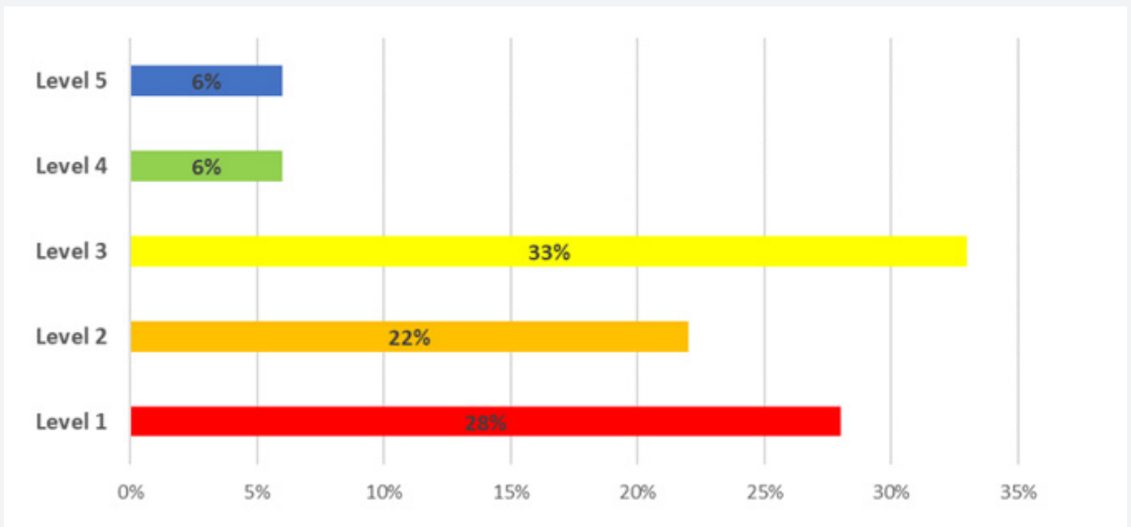


Figure 3: Rating of the current auditing/assessing method for Cybersecurity controls on ICS.

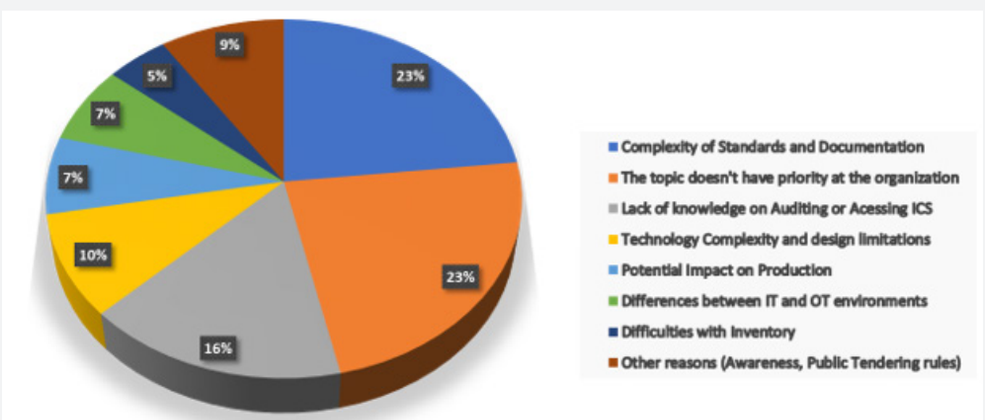


Figure 4: Main challenges on auditing/assessing heterogeneous ICS/SCADA implementations.

Research Findings

This findings from item B in regards the effectiveness of the existing method for assessing/auditing ICS Cybersecurity controls confirmed our assumption and demonstrates that not a lot has changed compared with the results from the ISACA Cybersecurity Survey performed in 2014 with 32 Dutch companies [4], according to the respondents "the most challenging topic in monitoring seems to be security testing and performing internal and external audits on a regular basis". Within the main challenges on auditing and assessing ICS Cybersecurity controls the "complexity of the standards and documentation" and "the lack of priority within the organization" scored 23% each, demonstrating a serious need to

i. Develop Cybersecurity skills and

ii. To ensure the proper governance around the Cybersecurity topic.

"Lack of knowledge on Auditing or accessing ICS" scored in 3rd place with 16%, showing that either company resources are not capable of auditing or assessing Cybersecurity controls, among the responses from the participants one in particular can illustrate the situation "Auditors don't have real knowledge about OT (Operational Technology) systems and their specific protocols," the results match recent studies about the shortage in Cybersecurity skills and its impact in all industry sectors, as highlighted by Oltsik [14] on his article published on the electronic magazine CSO Online in January this year, "Research suggests cybersecurity skills shortage is getting worse". Other challenges also referred were related to the "Technology Complexity and design limitation," and "Differences between IT and OT environment," followed by "Impact on Production," these challenges can be directly related to knowledge of ICS/SCADA Cybersecurity risks and security controls and a possible uncertainty of its potential impact on the production environment.

About possible opportunities for improvement on their audit/assessment process, Information Security Executives and ICS specialists, see opportunities mostly for

i. Identifying better ways to assess ICS/SCADA Risks,

ii. Looking for additional assurance and

iii. Through improvements related to the organization.

Basically these three suggestions are in complete resonance with the recent study published by the management consulting firm McKinsey [15], called "A new posture for cybersecurity in a networked world," according to the study, [16]"Successful cyber-strategies are built one step at a time, drawing on a comprehensive understanding of relevant business processes and the mind-set of prospective attackers. Three key steps are to prioritize assets and risks, improve controls and processes, and establish effective governance". Based on this analysis, we can list 5 Critical Success Factors to deploy an effective Cyber Assurance Model (Artefact 1)

i. Have the Buy in From the Organization Leadership?

ii. Invest on the Development of Cybersecurity Skills

iii. Define and Deploy Standards Aligned to the Organization Needs

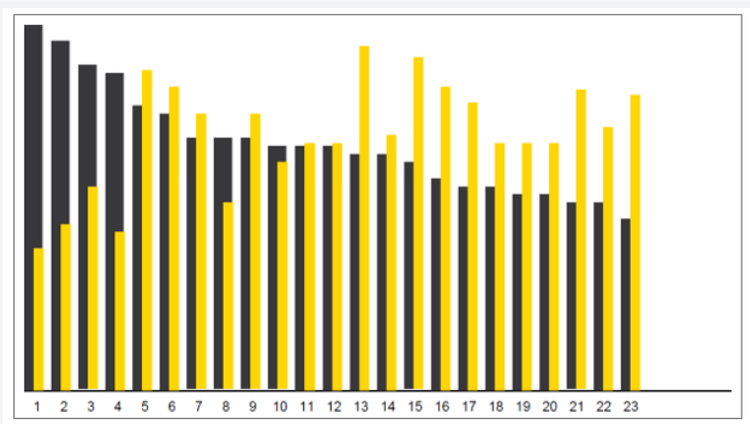
iv. Build a Multi-skilled Audit/Assessment Team

v. Ensure Identified Risks Are Properly Reported

Most Effective Ways to Report to the Board

Session with information security executives and ICS specialists

The Figure 5 lists all the inputs from the GSS session held with Information Security Executives and ICS Specialists in The Hague, the list brought valuable insights and the open answers provided by all the participants were compiled into an artefact that was later shared with C-Level Executives for their validation and comments.



#	Item	Rating	A	Variability	C
1	Terms in loss of money/imago damage	4.5		35%	
2	Translate issues to money, risks etcetera and responsibilities of the board	4.3		41%	
3	Talk about money (risks)	4.0		50%	
4	Link with strategy goals (free translation from "Koppelen aan strategische doelstellingen")	3.9		39%	
5	Define the level of related image/financial/personal risks when doing nothing	3.5		79%	
6	Damage to public image	3.4		75%	
7	Make remaining risks clear and have the board formally accept them	3.1		68%	
8	Are risks incidental or structural, relate to corporate interest	3.1		46%	
9	Show examples with lead to direct calls to the boards	3.1		68%	
10	via Corporate Internal Audit Office	3.0		56%	
11	Dashboarding KPI's	3.0		61%	
12	Reporting of real hacks and events and attempts that have occurred	3.0		61%	
13	Red Team demo	2.9		85%	
14	Benchmark	2.9		63%	
15	Through an Information Security Management System ISMS	2.8		82%	
16	Video presentation	2.6		75%	
17	Strong LoD 2 capability	2.5		71%	
18	Inspection of the whole chain from design till production (Free translation from:Rondgang in de keten. Van ontwerp tot productie)	2.5		61%	
19	Security reports	2.4		61%	
20	Similar reporting format on each company in the sector	2.4		61%	
21	Point to stuxnet	2.3		74%	
22	Full freedom (transparency), no filter from operation	2.3		65%	
23	Report on awareness campaigns (e.g. mandatory onboarding test for onboarding)	2.1		73%	

Figure 5: Input ISF's and ICS Specialist on most effective ways to report Cyber Risks to the Board.

Validation most effective ways to report ICS/SCADA cybersecurity risks to the board

In order to validate the inputs from the Information Security Executives and ICS Specialists, the results of the findings from the item A were separated in two categories, content "What to report to the board,"," and format "How to report to the board the two sets of data were sent to C-level executives for validation. At the C-level validation on what should be reported to the Board, Figure 6, the highest score twenty five(25), was given to "cybersecurity risks linked to the company strategy or corporate interest," the second highest score of twenty three (23) was given to "reported in terms of operational risks and impact," and the third highest score with twenty two (22) was given to "reported in terms of Financial and Image Risks," the report of cybersecurity risks "compared to other real events that affected the same or similar industries" and in format of KPI's had the lowest score, nineteen (19) and thirteen(13) respectively.

Figure 6: What to report to the Board in terms of Cybersecurity risks?

At the C-level validation of how Cybersecurity risks should be reported to the Board, Figure 7, the highest score twenty (20), was given to, "via reports from External Cybersecurity companies or Ethical Hackers" and "via Internal Audit Reports," the second highest score of eighteen (18) was given to "as Benchmark results," and the third highest scores, sixteen (16) was given to "Cybersecurity reports," fourteen (14) "via dashboard with KPI's," and reporting cybersecurity risks using a "video presentation" score the lowest seven (7).

Figure 7: How to report to Cybersecurity risks to the Board?.

Findings

The survey session performed with C-Level Executives to validate the most effective ways to report ICS/SCADA Cybersecurity Risks to the Board, has achieved its objective.

In terms of content on "What should be reported to the Board," the following options received a higher score (order of precedence), according to the C-Level executives:

i. In alignment with the company strategy or corporate interests,

ii. Related to Financial and image risks

iii. Reported in terms of operational risk and impact.

When asked about what kind of information/data/context should be included in a Cybersecurity report to the Board, the executives were emphatic about the need to report impact either operationally or financially, the high response rate on the Cybersecurity risks "aligned with company strategy or corporate interests," shows evidence that specific knowledge of that subject may contribute to the elaboration of the report and therefore to the presentation of results more aligned with the interests of the Board.

Additionally, in terms of format, on how Cybersecurity Risks should be reported, the following options received a higher score (order of precedence), according to the C-Level Executives:

i. Via Reports from eternal Cybersecurity companies

ii. Via Internal Audit

iii. In the format of Benchmark results

The answers from the senior leaders revealed although slightly different than the input of the Information Security Executives and ICS Specialists, emphasis in Benchmarking, references to other high- profile Cybersecurity events in the industry also appeared on their comments, the reference to the usage of KPI's although limited seemed still to be relevant for 33% part of the respondents.

*The fact Board members would have preference on receiving this information via Reports from external Cybersecurity companies or Internal Audit deserves further investigation; however, it needs to be put in the context of the closed questions and the limited options given to the executives on the survey.

Recommended Practices

The Figure 8 aims to provide a set of "Practices that can enable companies and institutions to effectively address Cybersecurity Risks on the Industrial Control System Environment," to be delivered as the main objective of this research, these practices are based on the review of existing literature and interviews with Information Security Specialists, ICS Practitioners, Security Officers, Academics and Board Members. This answers the main research question that was: "Why companies and institutions are failing to deploy Cyber Security Controls on Industrial Control Systems Environment, proposing practices that can enable them to effectively address Cybersecurity risks on the Industrial Control Systems environment?"

7 Practices to enable the efficient deployment of Cybersecurity controls on Industrial Control Systems

Practice	Objective
1- Ensure Cybersecurity Governance is defined and embraced by management	Cybersecurity must be an active part of the organization, established and supported by proper structure, processes and relational mechanisms
2- Define a Cybersecurity Program	Define the strategy to address Cybersecurity risks in alignment with the business goals and supported by people, processes and technology
3- Invest in the Development of Cybersecurity Skills	Ensure all personal in charge of deploying or maintaining cybersecurity controls receives appropriate training.
4- Choose for a suitable Risk Assessment methodology	Adopt or create a sounding Risk Assessment methodology aligned with the company Enterprise Risks Management.
5-Build a Multi-skilled Work Force	The complexity and integrations existent on industrial control systems demand for combined efforts among different specialists
6- Perform Regular Cybersecurity Assessments Using Multi-skilled Professionals	Define your assessment plans, define assessment goals and ensure assessments are performed according with a list of practices or working book.
7- Ensure Cybersecurity Risks are reported	Cybersecurity incidents can have serious impact on companies operation and eventually to lives, therefore reporting and tracking those incidents is fundamental.

Figure 8: Practices to enable the efficient deployment of Cybersecurity controls on ICS.

Limitations and Conclusion

Performing a study across between three distinct areas on knowledge and different industries, implies certain limitations which were addressed through the adoption of methods, procedures and tools to ensure the adherence to the required rigor demanded by design science. This research was carefully conducted to ensure all the data captured remains reliable and repeatable allowing a further extension of this research work, the GSS tool helped in documenting every step ensuring repeatability. This research was also time bounded, therefore the information connected here reflects the studies performed until this date.

In this research we were able to examine the reasons why companies and institutions are failing to deploy Cybersecurity controls in the ICS environment, that was only made possible thanks to the input of many professionals from Industrial Control Systems industry, Information Security Executives, Information Security Specialists, Assurance Professionals and Senior Leaders. X number of participants participated in this study. Looking back on the first readings about Cybersecurity incidents affecting Manufacturing, [15] and the Critical Infrastructure sector and the respective reasons attributed to these incidents, it is quite easy to draw conclusions and immediately affirm that many of those incidents were caused by poorly designed processes, outdated systems and lack of knowledge, exploited by all sort of threats ranging from viruses to hyper-skilled hackers. Besides of the Fear Uncertainty and Doubt (FUD) there's not a lot in terms of lessons learned from this events that could effectively help companies to protect against Cybersecurity threats.

The examination done with the practitioners shows that the effort in securing Industrial Control Systems against Cyber threats is still minimal, according with the practitioners, there is no priority set, lack of ownership, knowledge gap and a few participants have even mentioned "it is a lack of a big incident in here", emphasizing organizations are not paying attention on these risks, citing Rothrock [17], "Company leadership must have an unambiguous understanding of the key elements of security and resilience". According to 60% of the Practitioners, the number one barrier for deploying Security Controls on ICS environment is "Lack of Priority or Stakeholder involvement" and 4% of them affirm that is lack of Governance. Based on that, it's possible to affirm that companies should focus more in establishing a proper governance not only by defining priorities and attributing ownership but also by linking cybersecurity indicators to their safety and reliability targets.

Once responsibilities are clearer and priority is defined, it is necessary to define a strategy to tackle the problem what can be achieved with the help of a cybersecurity Program properly funded and supported, these two topics, Establishing Governance and Defining a Cybersecurity Program were included in the list of recommended practices and during the validation survey were both scored as Highly Effective or Effective by 81,3% of the respondents. Practitioners have also revealed concerns with the lack of specific ICS Security knowledge, what implies in not knowing how to make the ICS Secure, that was the answer from 25% of the respondents. During the validation survey, investments on developing cybersecurity skills was rated 43,8% as highly effective and 31,3% as effective by the respondents, 18,8% scored it Neutral and 6,3% Limited effective, that's possibly an indication that ICS Security education may not be effective if not addressed in parallel with Governance and a cybersecurity program; Another alternative could be hiring or outsourcing the cybersecurity tasks.

The examination on how companies are performing the assurance of Cybersecurity controls touched similar points as such as lack of skills or knowledge and lack of ownership; When asked on how the practitioners would rate their current assessment method, from 1- Not effective until 5 - Highly effective, 50% of the respondents have rated their current assessment methods as Not effective or as Limitedly effective, this discover is astonishing and supports the fact that companies cannot validate whether their Cybersecurity controls. The main solution for this problem may also reside with the "buy in" from the senior management one of the CSF rated as Highly effective by 56,3% and as Effective by 37,5% of the respondents, scoring higher than other identified CSF such as invest on development of Cybersecurity skills (Highly effective-18,8%, Effective-62,5%) and standards aligned to the organization needs (Highly effective-25%, Effective-43,8%) also had a good rate but were not considered as effective as the first one.

The main remaining questions for now seems "Why are companies and institutions not having the support from the executive leadership on securing their ICS environment?". To answer to this question, it's necessary to reflect on the need for creating demands or in other words, making the Senior Leadership aware of the need to improve cyber Security Controls, that can be done through the report and escalation of cybersecurity risks to the senior leadership or as a requirement from any country specific law and regulation, the interviews with Board members revealed they're interested in hear about Cybersecurity risks, in terms of regulations the North American cybersecurity security framework, Obama [18], does not make any impositions on the need to protect critical infrastructure, since its adoption is voluntarily. Overall, implementing strong cybersecurity controls requires business involvement through proper governance, levels of security technology, management, education skills and vigilance that go far beyond the demands of regulatory compliance, complementing what Franken [4] states on the ISACA paper Governance of cybersecurity.

Acknowledgement

None.

Conflict of Interest

No conflict of interest.

References

1. Auffret JP, Jane l Snowdon, Angelos Stavrou, Jeffrey katz, Diana Kelley, et al. (2017) Cybersecurity Leadership: Competencies, Governance, and Technologies for Industrial Control Systems. Journal of Interconnection Networks 17(1).
2. Nicholson, S Webber, S Dyer, T Patel, H Janicke (2012) "SCADA security in the light of Cyber-Warfare," Computers & Security 31(4): 418-436,
3. Fitzgerald T J (2017) ISACA – Auditing Cybersecurity: Evaluating Risk and Auditing Controls, ISACA.
4. Franken W, Fabri M Vlaanderen K (2014) ISACA Governance of Cybersecurity, ISACA Chapter NL.
5. Yuri Bobbert (2017) On Exploring Research Methods for Business Information Security Alignment and Artefact Engineering. International Journal of IT/Business Alignment and Governance 8: 28-41.
6. CNPI (2015) Security for Industrial Control Systems- Establishing ongoing governance, A Good Practice Guide.
7. Harrell B (2018) Improving cybersecurity governance in the boardroom.
8. Alqirem, Raed (2003) A Viable System Model to Analyze an Organization's Metasystem.

9. Von Solms R (2009) Information Security Governance. ISBN 978-0-387-79984-1.

10. Chang Shuchih Ernest, Ho Chienta (2006) Organizational factors to the effectiveness of implementing information security management. Industrial Management and Data Systems.

11. Windelberg Marjorie (2015) Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection.

12. ENISA (2011) Protecting Industrial Control Systems, recommendations for Europe and Member States.

13. Cherdantseva Yulia, Burnap Pete, Blyth Andrew, Eden, Jones, et al. (2016) A Review of cyber security risk assessment methods for SCADA systems. Computers & Security 56: 1-27.

14. Oltsik, J (2018) Research suggests cybersecurity skills shortage is getting worse.

15. Mckinsey (2018) A new posture for cybersecurity in a networked world.

16. Rothrock RA, Kaplan J, Van der Oord E (2017) The board's role in managing cybersecurity risks. MIT Sloan Management Review.

17. Lee R M, Assante M J, Conway T (2014) SANS Institute, ICS defense.

18. Obama Barack (2013) Executive Order – Improving Critical Infrastructure Cybersecurity.