Cybersecurity Awareness in an Industrial Control Systems Company

Stefan Prins[1], Annlizé Marnewick[1] & Suné von Solms[2]
[1]Postgraduate School of Engineering Management
[2]Department of Electrical Engineering Science
University of Johannesburg
South Africa
svonsolms@uj.ac.za

Abstract: This paper investigates the cybersecurity awareness levels of employees at an industrial control systems organization and measures their knowledge on the potential impact of cyber-related attacks on their systems through a case study. Attacks on industrial control systems as well as the information technology infrastructure which it relies on, are becoming a growing problem for governments and organizations. Cybersecurity policies of organizations are critical to ensure that industrial control systems environments are adequately protected. It is equally important for the organizations to ensure that their employees are aware of the cybersecurity policies and why they must be implemented. In many cases, however, organizations are faced with employees who are not aware of the potential cyber-related security threats posed to their industrial control systems, nor the impact these attacks might have. Results show that although employees understand the severity of cyber vulnerabilities their awareness is low.

Keywords: Awareness, Cybersecurity, Industrial control systems, Vulnerabilities

1. Introduction

Individuals as well as organizations rely on information technology (IT) to assist them in their daily activities using equipment such as computers. Connected systems carry the risk of various cyber-related attacks, ranging from theft of data, personal information exposure, financial loss, sabotage to name a few. In the Industrial Control Systems (ICS) environment, the control systems are becoming more integrated with IT technology, which means that ICS systems are also more susceptible to cyber threats (Byres & Lowe, 2018). Organizations with highly connected ICS are faced with risks as attacks on these systems can have severe effects on the operations of the company. The data shows that cyber-related attacks on ICS systems are on the rise (Byres & Lowe, 2018). In 2017, the WannaCry worm infected Windows based computers and caused worldwide disruption (Symantec Security Response, 2017). The Stuxnet worm was designed to attack specific ICS systems, such as supervisory control and data acquisition (SCADA) as well as programmable logic controller (PLC) systems, and is considered as a weapon of cyberwarfare by some specialists (Singer, 2015). In 2015, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) discovered the BlackEnergy malware on computers of a Ukrainian power utility after the company had unscheduled power outages impacting many of their customers. The findings indicated that the intruder used remote access to infiltrate the network (ICS-CERT, 2018). The risk and vulnerability for ICS networks as well as the challenge to address these were discussed by the authors (Pretorius & van Niekerk, 2016). The head of global research and analysis at Kaspersky in the Middle East, Turkey and Africa stated that one of the biggest trends in Africa in 2018 was increased cyber-attacks on ICS and critical infrastructure systems (Smith, 2019).

Organizations must reassess their risks and consider strategies such as protecting the systems with multiple layers of security (Thomson, & von Solms, 2006). The practice of cybersecurity is there to protect the IT systems of an organization by preventing data breaches, forming part of business operations (Thomson & von Solms, 2006). Businesses in the ICS environment can no longer consider cybersecurity practice as a low priority and must change their position on how to deal with it in better ways to protect a critical system (Knowles et al, 2015). Governments from developed countries such as the United States (US) and United Kingdom (UK), developed cybersecurity policies to make their citizens more knowledgeable about cybersecurity. In South Africa, however, many companies lack cybersecurity policies and awareness relating to Industrial Control Systems security, amongst others. According to a study by Nexia International, 39% of South African organizations do not provide any training in cybersecurity, and only 30% train their employees occasionally (Nexia International, 2017). The South African government developed a cybersecurity policy, but the policy is unclear how the nation will be made aware of cybersecurity (Kortjan & von Solms, 2013).

The threats which exist in the domain of cyberspace is an increasing problem for organizations in the ICS environment and thus creates a situation where organizations must implement strategies to counteract the threats like educating the employees through awareness programs. This research aims to determine the level of cybersecurity awareness in the organization in the ICS environment and to determine the impact of the potential risk for the organization. This paper is structured as follows: Section 1 provided the introduction where section 2 provides an overview on the related work. section 3 describes the research methodology followed in this research. Sections 4 and 5 provides the Data Collection and Results sections, respectively. Section 6 includes a discussion and section 7 concludes this paper.

2. Related Work

Industrial Control Systems is a term used to refer to the overall use of control systems (Stouffer et al, 2015). It is common to see terms such as ICS or SCADA interpreted as the same thing, but in reality, the terms refer to different types of control systems (Krotofil & Gollmann, 2013), where ICS is viewed as covering all types of systems. ICS used to be a complex system designed for dependability, durability, and safe to use by operators (Krotofil & Gollmann, 2013). These type of design characteristics allowed the control system to function separately from any other systems with the minimum risk. Through the evolution of technology in the ICS environment, the IT infrastructure started to become more integrated with the control systems and replacing or enhancing some of the other physical systems (Stouffer et al, 2015). According to (Krotofil & Gollmann, 2013), the evolution of technology allows for better integration with other systems and integration with cyber systems. The evolution of technology improves the efficiency of the systems, but it also causes more risk which is difficult to foresee (Krotofil & Gollmann, 2013).

ICS systems require companies with the right set of knowledge and skills to develop a system according to the requirements of the client and who can support the ICS system through its product lifecycle. Cyber attackers have learned of the value of targeting ICS as it can lead to severe damage to daily business operations, including operational shutdowns, equipment damage, financial loss, intellectual property loss, as well as health and safety risks (TrendMicro, 2016). In order to secure ICS infrastructure, personnel, policy makers and engineering experts must be involved to determine and analyze ICS infrastructure risks. The cybersecurity maturity level of an ICS organization is dependent on how well it understands its ICS and network environments. In the context of more connected systems and the evolution of ICS to be fully connected, developers, users and support personnel must therefore have the knowledge and understanding of the threats, vulnerabilities and risks that come with the technology and must grasp the idea of how to implement cybersecurity.

Commenting on the increase in cyber-related attacks on ICS in Africa, the head of global research and analysis at Kaspersky in the Middle East, Turkey and Africa stated that “(i)n many countries – especially in Africa – there is a lack of awareness of this threat to critical infrastructure. Many of these facilities are not aware that they are exposed to cyber risk and can be controlled if hacked” (Smith, 2019). According to Kortjan & von Solms (2013), governments and organizations must use policies to ensure that the desired goals, such as employee awareness, are met. Management of an organization should ensure the workers follow the company policies. Company policies must set out what the cybersecurity procedures are and must then be used to control the worker's behavior towards cybersecurity. A cybersecurity policy of an organization must enable the workers to be more aware when using company information or assets and help to protect the company from potential damages (Vroom & von Solms, 2002). Companies must run their awareness programs on a regular basis to ensure the culture remains intact (von Solms & von Solms, 2004). Awareness programs help the workers understand the technical insights and how procedural processes can be used to prevent cybersecurity attacks in the ICS environment. Awareness programs in an organization are there to continuously drive the importance of cybersecurity and can't be considered as a quick fix. In addition, ICS cybersecurity awareness programs must also be adapted from IT because of the different characteristics (Stouffer et al, 2015) and must form part of the policies of an organization or government (Byres & Cusimano, 2012). To increase awareness, programs to inform workers about the threats, vulnerabilities and risks in the ICS environment should continuously be integrated with organizational communication drives.

Similar to awareness programs, an organization must develop a plan to improve a workers’ skills in cybersecurity through training programs. The training programs must build and enhance the skills of the workers. In addition, the ICS and IT communities in an organization must form a good working relationship.

Management in organizations must ensure the two different groups can work together and ensure there is knowledge transfer between the groups. Sharing knowledge between the two groups will allow better solutions, better use of workers, and better use of monetary resources (National Cyber Security Centre, 2015). Piggin (2013) identified 14 security themes that leads to specific challenges when ICS and SCADA systems are integrated into organisations business environments (Piggin, 2013). Two of the themes relates to the awareness as displayed in Table 1.

Table 1: Cyber security themes

Theme	**Information technology**	**Industrial control system**	**Challenge**
IT	Good	Generally a poor understanding of cyber security	Control engineers generally lack cyber security education or training
ICS	A poor understanding of control systems operating environments	Recently events have started to raise more awareness but lack of implementation.	Knowledge often limits required understanding to implement security. Fragmented team leads to potential security weaknesses.

Although security priorities within an ICS landscape is different from traditional IT landscapes, these two are integrated and cannot be addressed separate from each other in ICS implementations. From Table 1 it can be seen that a low level of cybersecurity awareness in the ICS environment can lead to cyber-related challenges. The requirements of a higher level of cybersecurity awareness by control systems engineers is therefore highlighted in (Piggin, 2013). Cybersecurity awareness in an organization is critical, as human error due to a lack of cybersecurity knowledge and awareness is one of the leading cause of cyber-incidents (Kaspersky, 2019). A framework for improving awareness and skills of employees' in organizations by (Torten, Reaiche & Boyle, 2018) suggested three parallel approaches:

1. Increase ongoing awareness by implementing awareness programs.
2. Establish training frameworks and focus on countermeasure training.
3. Continuously evaluate program effectiveness.

To determine the potential risks faced by an ICS organization, this paper investigates the cybersecurity awareness of employees of an ICS organization in South Africa. The methodology followed in this investigation is detailed in the next section.

3. Methodology

The aim of this research is to determine the level of cybersecurity awareness and the level of impact thereof for the organization. A case study was used as it is ideal to gain an in-depth understanding of a problem (Zikmund et al, 2010). The organization researched in the case study is a small South African company which specializes in the ICS environment by providing solutions, products, and services for the industrial market. The employees of the organization are typically involved in designing, implementation, commissioning, and maintenance of control systems for industrial customers. The employees' level of cybersecurity awareness and their perceived level of impact regarding risks were the unit of analysis in this research. The case study data collection made use of a questionnaire and document analysis to get the necessary information so that the researchers can determine the current condition within the organization. The study groups in the organization included the service department, project department, and internal sales department. The occupational respondents included the engineering manager, systems engineers, service engineers, and internal sales. As a small company, the number of professionals in these positions totals 10. The questionnaire was electronically distributed to all the identified respondents (total of 10) as a PDF form.

During the data collection process, the purpose was to collect the following data: (i) the participant's knowledge of cybersecurity awareness and (ii) the participant's perceived level of impact regarding risks. To assess these levels, a Likert scale was used as the measuring instrument to determine each respondent's knowledge of cybersecurity awareness and perceived level of impact. Table 1 illustrates the two Likert scales used for each statement testing knowledge of cybersecurity awareness and perceived level of impact.

Table 1: Likert scales for questionnaire

	1	2	3	4	5
Knowledge of cybersecurity awareness	Not aware	Somewhat	Moderately	Extremely	

		aware	aware	aware	
Perceived level of impact	No impact	Minor impact	Moderate impact	Significant impact	Severe impact

Multiple data sources were used to triangulate the results of this study. The following data were utilized:

1. Benchmark data was collected which categorized vulnerabilities into different groups to present the different vulnerabilities of the ICS environment from the literature (Stamp, Young & Mae Depoy, 2003).
2. Document analysis related to the organization in the ICS environment is measured against the benchmark data collected in step 1. Organizational documents were divided according to the categories identified in the benchmark data.
3. Data collection though a questionnaire, collecting data on the level of awareness and the level of perceived impact from the participants. The structure of the questionnaire was derived from the benchmark data collected in step 1.

The common vulnerabilities as identified from the Guide to Industrial Control Systems (ICS) Security by the National Institute of Standards and Technology (NIST) was categorized into these different groups and was used as the benchmark data, shown in Table 2 (Stouffer et al, 2015). This list of vulnerabilities was the basis used in the questionnaire design as well as the document analysis checklist.

Table 2: Vulnerability statements per ICS dimension

Data	
Data 1	Data is not correctly classified according to the sensitivity categories of industrial control systems.
Data 2	Sensitivity categories are not determined according to the level of impact.
Security administration	
Security admin 2	No adequate security policies for ICS such as config management, access control, and authentication.
Security admin 2	There are no official awareness and training programs about cybersecurity in industrial control systems.
Security admin 3	There is a lack of or no implementation guides on industrial control systems equipment.
Security admin 4	Organizational mechanisms are absent for security policy enforcement.
Security admin 5	The effectiveness of the security controls is not adequately reviewed.
Security admin 6	Inadequate security plans for ICSs, contingency plan, incident detection plan and response plan, not used.
Networks	
Networks 1	Data flow control is not utilised between systems such as the ICS and business networks.
Networks 2	Firewalls are not used between networks or not configured correctly.
Networks 3	There exist no adequate firewall and router logs for the industrial control system.
Networks 4	Standard, well-documented communication protocols are used in plain text.
Networks 5	Authentication of users, data, or devices of an industrial control system is substandard or non-existent.
Networks 6	Unsecured industrial control system protocols with no integrity checking for communications are utilised.
Networks 7	Inadequate authentication and data protection between wireless connections and access points.
Architecture	
Architecture 1	The addition of security controls into the architectural designs of ICS are inadequate.
Architecture 2	Insecure modifications are allowed to the architecture of industrial control systems.
Architecture 3	Non-control traffic allowed on the control network of industrial control systems.
Architecture 4	Control network services such as a domain controller are not controlled within the control network of ICS.
Architecture 5	Redundant components used for critical functions are absent from industrial control systems.
Platforms	
Platforms 1	Modifications of hardware, software, and firmware of industrial control system are not properly managed.
Platforms 2	There exist delays in OS and vendor software patches for the industrial control systems.
Platforms 3	Security patches are not maintained for industrial control systems.
Platforms 4	Security changes are not tested adequately before implementation.
Platforms 5	Poor remote access controls to access the industrial control systems are utilised
Platforms 6	Default or poor configurations on the industrial control platforms are implemented.
Platforms 7	Critical configurations of industrial control systems are not stored or backed up.
Platforms 8	There exist no data encryption on portable devices for the added protection.
Platforms 9	Password implementation policy is not implemented according to the organizational policies.
Platforms 10	Strong access controls are not applied across industrial control systems.
Platforms 11	Improper sharing methods are used to replicate data to other systems.
Platforms 12	Anti-malware software is not installed or updated on platforms.
Platforms 13	Anti-malware is loaded on platforms without adequate testing.

Platforms 14	Software on industrial control platforms are vulnerable to denial of service attacks.
Platforms 15	Intrusion detection or prevention software on industrial control platforms are not installed.
Platforms 16	Logs from industrial control systems are not collected or examined.
Platforms 17	Unauthorised access to the physical equipment is allowed.
Platforms 18	Physical ports on industrial control platforms are not secured.
Platforms 19	Data on industrial control platforms are not adequately validated.
Platforms 20	Security capabilities installed on industrial control platforms are not activated.
Platforms 21	There exists inadequate user authentication, access privileges, and access control in the software.

It can be seen from Table 2 that 41 vulnerabilities falling within 5 categories were identified. These vulnerability statements were utilized as the baseline data for the data collection discussed in Section 4. In order to obtain information from the organisation's documentation, every identified vulnerably listed in the table above was compared it to the organisation's documents. When a document was found where the vulnerability was addressed, the document was recorded.

4. Data Collection

The organization in the ICS environment are measured against the benchmark data collected in step 1. The document analysis as well as the questionnaire design are discussed below.

4.1 Document Analysis

As part of the case study, documents were reviewed to determine how the organizational policies, guidelines and procedures addresses the ICS vulnerabilities. The documents investigated were the documents used by the organization to reduce the vulnerabilities and increase the security of the ICS environment. The organizational documents, which includes policy documents, guidelines and specification documents, are mainly used by the employees in ensuring the ICS infrastructure is protected and explain the processes to protect the products from cyber threats. The documents surveyed were the following:

1. Functional design specifications
2. Security countermeasures
3. Security guide
4. Security Requirements

Byres and Cusimano (2012) recommends a risk assessment to identify vulnerabilities in the ICS environment. Following this guideline, the document review was used to determine whether the organization is addressing these vulnerabilities. The organization documents were divided according to the categories identified in the benchmark data in Table 2. Every vulnerability identified in the benchmark data were compared it to the organization's documents.

4.2 Questionnaire

The respondents identified in the case study were asked to indicate their role in the organization. The aim of the question was to determine the demographics of the roles in the organization. The collected data were summarized in Table 3 to indicate the roles in the organization.

Table 3: Respondents' role in ICS organization

Respondent role	Number of respondents
Engineering Manager	1
Service Engineer	5
Systems Engineer	2
Project Manager	1
Internal Sales	1

The benchmark data of ICS vulnerabilities from Table 2 was used to develop the list of statements for measuring the participants. The validity of the questionnaire was obtained by building research questions, case study proposition and principles on the benchmark data shown in Table 2. Reliability was achieved using the stated data collection procedures and the case study database. The questionnaire was divided into two main sections, detailed below.

Cybersecurity awareness: The questionnaire's first objective was to determine the respondent's level of awareness. The questionnaire was designed to measure awareness of the vulnerabilities using a 4-point Likert scale (not aware, somewhat aware, moderately aware and extremely aware). The respondents indicated their awareness of each vulnerability statement identified in the benchmark data. To measure the cybersecurity awareness, the question was stated as follows "How aware do you rate yourself for each statement".

Cybersecurity impact: The second objective of the questionnaire was to determine the level of impact of each vulnerability statement. The questionnaire was designed to measure the impact of vulnerabilities using a 5-point Likert scale (no impact, minor-impact, moderate impact, significant impact and severe impact). The respondents indicated the level of impact for each vulnerability statement. To measure the impact, the question was as follows "What level of impact do you rate each vulnerability statement".

5. Results

The results obtained from the document analysis and the questionnaires are discussed in the sections below. The calculated weighted average for each vulnerability element in the benchmark data was calculated. A weighted average was also determined per category.

5.1 Document Analysis

The document analysis shows that there are five areas which are not covered in the ICS organization's policies and governance documents. The vulnerability descriptions which are not addressed in the document are shown in Table 5.

Table 5: Unaddressed elements in document analysis

Element	**Description**	**Document analysis**
Data 1	Data is not correctly classified according to the sensitivity categories of ICS.	No
Data 2	Sensitivity categories are not determined according to the level of impact.	No
Security admin 4	Organizational mechanisms are absent for security policy enforcement.	No
Architecture 4	Control network services such as a domain controller are not controlled within the control network of ICS.	No
Platforms 2	There exist delays in OS and vendor software patches for the ICS.	No

Of the 41 vulnerabilities analyzed, only five were not documented in the company documents. The organization therefore understand the vulnerabilities. It can be seen that the vulnerabilities not addressed in the documents relates to all the vulnerability categories determined in the benchmark data, which includes Data, Security Administration, Architecture and Platforms.

5.2 Cybersecurity Awareness

The data collected in the first section of the questionnaire was analyzed to determine the weighted totals for each vulnerability statement. The weight mean was calculated in order to rank the responses (Robson & McCartan, 2016) . The vulnerability statements were ranked based on a weighted mean to determine the lowest to highest level of awareness based on weighted averages determined. If the weighted average was found to be lower or equal to 2.7, it was considered as low awareness. The 14 elements rated for low awareness are displayed in Table 6. The weighted average column of each vulnerability statement is displayed in a greyscale to indicate the level of awareness amongst respondents.

Table 6: Level of awareness (lowest rankings)

Element	**Description**	**Awareness Level**
Network 7	There exist inadequate authentication and data protection between wireless connections and access points.	2.3
Network 4	Standard, well-documented communication protocols are used in plain text.	2.4
Platforms 19	Data on industrial control platforms are not adequately validated.	2.5
Security admin 4	Organizational mechanisms are absent for security policy enforcement.	2.6
Security admin 6	Inadequate security plans for industrial control systems such as a contingency plan, incident detection plan and response plan, are not used.	2.6
Network 3	There exist no adequate firewall and router logs for the industrial control system.	2.6

Architecture 4	Control network services such as a domain controller are not controlled within the control network of industrial control systems.	2.6
Platforms 6	Default or poor configs on the industrial control platforms are implemented.	2.6
Security admin 2	No official awareness and training programs about cybersecurity in ICS.	2.7
Security admin 3	There is a lack of or no implementation guides on ICS equipment.	2.7
Security admin 5	The effectiveness of the security controls is not adequately reviewed.	2.7
Architecture 5	Redundant components used for critical functions are absent from ICS.	2.7
Platforms 4	Security changes are not tested adequately before implementation.	2.7
Platforms 20	Security capabilities installed on industrial control platforms are not activated.	2.7

It can be seen from the results in Table 6 that the lowest awareness items are distributed across Network, Platforms, Security administration and Architecture. If the weighted average was found to be higher or equal to 3.1, it was considered as high awareness. Twelve of the 41 vulnerabilities were rated with awareness above 3.1 out of a scale of 4 and are shown in Table 7.

Table 7: Level of awareness (highest ranking)

Element	Description	Awareness Level
Network 1	Data flow control is not utilised between systems such as the ICS and business networks.	3.5
Network 2	Firewalls are not used between networks or not configured correctly.	3.4
Platforms 1	Modifications of hardware, software & firmware of ICS not properly managed.	3.4
Platforms 17	Unauthorised access to the physical equipment is allowed.	3.4
Platforms 2	There exist delays in OS and vendor software patches for the ICS.	3.3
Platforms 14	Software on IC platforms are vulnerable to denial of service attacks.	3.3
Platforms 3	Security patches are not maintained for industrial control systems.	3.2
Platforms 15	Intrusion detection or prevention software on IC platforms are not installed.	3.2
Network 5	Authentication of users, data, or devices of ICS is substandard or non-existent.	3.1
Architecture 2	Insecure modifications are allowed to the architecture of ICS.	3.1
Platforms 10	Strong access controls are not applied across industrial control systems.	3.1
Platforms 13	Anti-malware is loaded on platforms without adequate testing.	3.1

The other vulnerabilities were all rated between 2.8 and 3. In total 29 vulnerabilities rated below 3.1, which translates to 71% of the vulnerabilities that have a low awareness. Six of the 8 vulnerability items with low awareness in Table 6 are mentioned in the company's documentation. Therefor the vulnerabilities are known in the organisation. However, the results show that the staff's awareness levels are low. As shown in Table 5, no documentation is available on Security administration 4 & Architecture 4.

5.3 Cybersecurity Impact

The data collected in the questionnaire related to the respondents' views on the possible impact for each vulnerability statement were analyzed to determine the weight mean per vulnerability. The vulnerability statements were ranked based on weighted mean to determine the highest level of impact based on the results of the respondents. If the weighted average was found to be higher or equal to 4.2, it was considered as high impact. The 15 vulnerability elements with the highest rated impact is displayed in Table 8. The weighted average column of each vulnerability statement is displayed in a greyscale to indicate the level of impact rated amongst respondents.

Table 8: Level of impact

Element	Description	Impact Level
Platforms 17	Unauthorized access to the physical equipment is allowed.	4.7
Security admin 1	There does not exist adequate security policies for industrial control systems such as configuration management, access control, and authentication.	4.6
Platforms 7	Critical configurations of industrial control systems are not stored or backed up.	4.6
Platforms 12	Anti-malware software is not installed or updated on platforms.	4.6
Security admin 3	There is a lack of or no implementation guides on ICS equipment.	4.5
Architecture 2	Insecure modifications are allowed to the architecture of ICS.	4.5
Platforms 15	Intrusion detection or prevention software on IC platforms are not installed.	4.5
Network 6	Unsecured ICS protocols with no integrity checking for communications are used.	4.4
Platforms 5	Poor remote access controls to access the industrial control systems are utilised	4.3

Platforms 10	Strong access controls are not applied across industrial control systems.	4.3
Security admin 2	There are no official awareness and training programs about cybersecurity in ICS.	4.2
Network 5	Authentication of users, data, or devices of an ICS is substandard or non-existent.	4.2
Architecture 5	Redundant components used for critical functions are absent from ICS.	4.2
Platforms 1	Modifications of hardware, software, and firmware of ICS not properly managed.	4.2
Platforms 21	Inadequate user authentication, access privileges & access control in software.	4.2

It can be seen from the results in Table 8 that the vulnerability elements rated as having the highest impact is all covered in the policy documents. Elements from the Platform and Security Architecture ICS dimensions are most prevalent in the top 10 rankings. The respondents rated 21 of the vulnerabilities to have an impact higher than 4 out of a 5 point scale, and 15 of the vulnerabilities had an impact between 3.8 and 3.3.

6. Discussion

Figure 1 shows the normalized weighted averages for all 5 ICS dimensions. When comparing the overall in terms of the 5 ICS dimensions, it can be seen that security administration and architecture dimensions had the lowest weighted averages for awareness amongst respondents. These two ICS dimensions also shows high ratings of impact, where Security Administration obtained the highest rating for impact of the ICS dimensions. Security administration also has one vulnerability element (Security Administration 4) which was not covered in the organization's documentation.

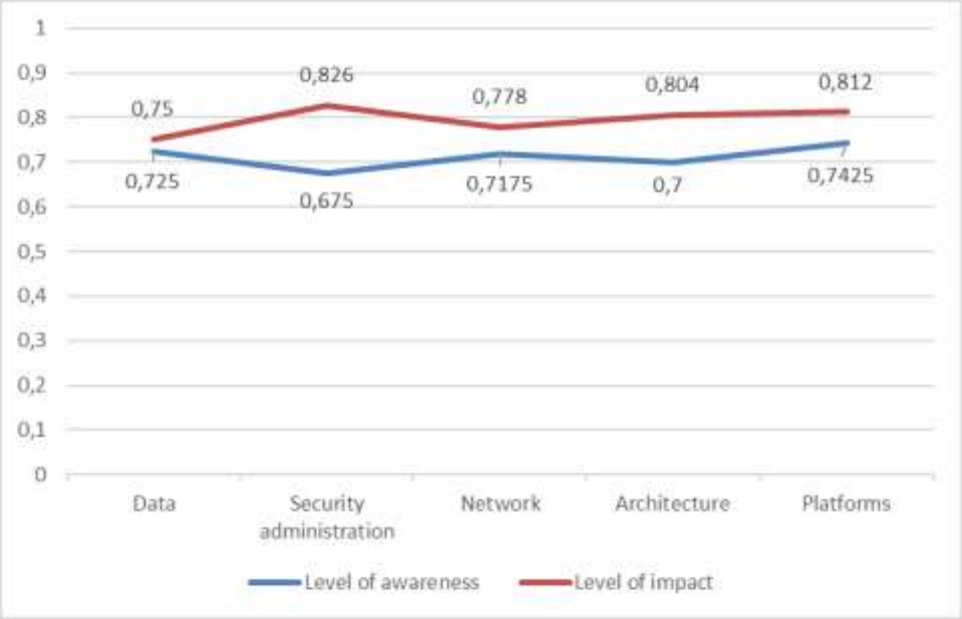

Figure 1: Awareness and Impact for the 5 ICS dimensions

The security administration involves the organization's policies and procedures which are used to address the security vulnerabilities in the ICS environment. The potential cause for a low awareness can be attributed to little or no training in the organization's cybersecurity policies and procedures. When looking at the results of the respondent's background information, it can be seen that the majority of the respondent's role in the organization is engineering driven in the ICS environment. The security administration in the organization is an administrative activity and could be a weakness for the engineers. The dimension with the highest level of impact was the security administration. This means that the respondents consider the security administration to have the biggest impact on the organization's operational function and that it is recognized as a problem by the respondents. Comparing the low level of awareness to the large impact of security administration as indicated by the respondents, it is evident that the security vulnerabilities pose a risk and that awareness for this dimension should be a top priority for the organization.

The data dimension was considered by the respondents to have the lowest impact on the organization. This means that respondents may not realize how important it is to protect the data infrastructure in the ICS environment, which can pose a danger to the operations of the organization.

7. Conclusion

This paper investigated the cybersecurity awareness levels of employees at an ICS organization in South Africa and measured their knowledge on the potential impact of cyber-related attacks on their systems through a case study. In this case study, benchmark data was collected from the literature to categorize vulnerabilities 5 dimensions of the ICS environment. This data was used to create a questionnaire to collect data on the level of awareness and the level of impact from employees of an ICS organization. The benchmark data was also used determine the documentation that the organization has relating to the benchmark ICS vulnerabilities.

Industrial control systems are becoming more integrated with supporting IT technologies, which means that ICS systems are also becoming more susceptible to cyber-related attacks, including theft of data, personal information exposure, financial loss and sabotage. These attacks can have severe effects on the operations of the organizations. Cybersecurity policies of organizations as well as cybersecurity training relating to these policies are critical factors to ensure that the ICS environments in organizations are adequately protected. There exist cases, such as the case study presented in this research, where organizations have employees who understand the severity of cyber vulnerabilities, however, their awareness is low. In addition, companies might not have adequate cybersecurity training programs.

As case study was conducted on a small ICS organisation in South Africa, the results are not generalisable, but does provide an indication of the shortcomings many small ICS organizations may face. A shift is required in organizations to move from a governance checklist to a cybersecurity culture. This shift should be facilitated though communication programs, followed up by training programs and a continuous monitoring of these to establish a cybersecurity culture. In addition, it can be recommended that the management of small companies start to take responsibility in enforcing the cybersecurity policies and guidelines and keep track thereof. The employees will start to improve their cybersecurity by becoming more knowledgeable about the cybersecurity policies and procedures of the organisation.

References

Byres, E. and Cusimano, J. (2012) “7 Steps to ICS and SCADA Security”. Tofino Security. Available at: https://www.tofinosecurity.com/sites/default/files/WP-7-Steps-to-ICS-Security.docx.

Byres, E. and Lowe, J. (2004) “The myths and facts behind cyber security risks for industrial control systems”. VDE Kongress, pp 213-218.

ICS-CERT. (2018) “Cyber-Attack Against Ukrainian Critical Infrastructure”. Available at: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (Accessed: 16 April 2019).

Kaspersky. (2019) “Kaspersky Industrial Cybersecurity Training Program Training with Kaspersky Lab ICS CERT”.

Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. and Jones, K. (2015) “A survey of cyber security management in industrial control systems”. International Journal of Critical Infrastructure Protection, 9, pp 52-80.

Kortjan, N. and von Solms, R. (2013) “Cyber Security Education in Developing Countries: A South African Perspective”. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 289-297.

Krotofil, M. and Gollmann, D. (2013) “Industrial control systems security: What is happening?”. 11th International Conference on Industrial Informatics (INDIN), IEEE, Bochum, Germany, pp 670-675.

National Cyber Security Centre Security for Industrial Control Systems. (2015) “Improve Awareness and Skills - A Good Practice Guide”. Available at: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/SICS - Improve Awareness and Skills Final v1.0.pdf.

Nexia International. (2017) Global Cybersecurity Report. URL Available at: https://www.cohnreznick.com/-/media/resources/global_cybersecurity_report_2017.pdf (Accessed: 15 April 2018).

Piggin, R.S.H. (2013) “Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security”. in IET Conference on Control and Automation 2013: Uniting Problems and Solutions, pp 1-6.

Pretorius, B. and van Niekerk, B. (2016) “Cyber-security for ICS/SCADA: a South African perspective”. International Journal of Cyber Warfare and Terrorism, 6 (3), pp 1-16.

Robson, C. and McCartan, K. (2016) “Real World Research”. Wiley.

Singer, P.W. (2015) “Stuxnet and its hidden lessons on the ethics of cyberweapons Case”. Western Reserve Journal of International Law, pp 79.

Smith, C. (2019) “Major spike in SA cyber attacks, over 10 000 attempts a day - security company”. Fin 24.

Stamp, E., Young, Y., and Mae Depoy, J. (2003) “Common vulnerabilities in critical infrastructure control systems”. Sandia National Laboratories.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. and Hahn, A. (2015) “Guide to Industrial Control Systems (ICS) Security”. National Institute of Standards and Technology (NIST).

Symantec Security Response. (2017) “What you need to know about the WannaCry Ransomware”. Available at: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.

Thomson, K.-L., von Solms, R. and Louw, L. (2006) “Cultivating an organizational information security culture”. Computer Fraud & Security, 10, pp 7-11.

TrendMicro. (2016) “Securing ICS environments in a connected world”. Available at: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/securing-ics-environments-in-a-connected-world

Von Solms, R. and von Solms, B. (2004) “From policies to culture”. Computers & Security, 23 (4), pp 275-279.

Vroom, C. and von Solms, R. (2002) “A Practical Approach to Information Security Awareness in the Organization”. in Ghonaimy, M.A., El-Hadidi, M.T. and Aslan, H.K. eds. Security in the Information Society: Visions and Perspectives, Springer US, Boston, MA, pp 19-37.

Zikmund, W.G., Babin, B.J., Carr, J.C. and Griffin, M. (2010) “Business Research Methods”. South-Western, Cengage Learning.