Industrial Control Systems Protection Survey

Belgium 2014

Written by Stephen Smith
Reviewed by Anja Van Geert

ONRIX

Table of contents

Introduction

The realization of potential threats to digital devices and systems is unavoidable once one is involved in supporting people and organisations to mitigate these risks. There is a rapid conscious realisation that the effort required is greater than the acceptance of the real threat recognition within most organisations. It is this thought coupled with other survey examples, such as the SANS SCADA and Process Control Security Survey*, that triggered my interest into understanding local maturity and preparedness against such risks. I just became curious about the Belgian situation and decided to better comprehend and eventually raise awareness.

Industrial control systems (ICS) is a term utilised to describe digital systems used in production environments. Such systems are generally used to control and supervise operational activities. These system are also used to monitor alarms systems, security systems and a host of other functions. ICS are becoming progressively more dependent on "standard" IT technologies; technologies such as Microsoft Windows, TCP/IP, web browsers and wireless technologies, are replacing conventional "proprietary" systems. Older proprietary industrial systems are being either replaced or boosted with "off the shelf" software. Many of the standard IT security protection measures are difficult to apply in industrial control environments. Therefore, there may be insufficient security measures present to protect control systems and keep the environment safe and secure.

Today, Windows XP is still widely used in industrial environments. The demise of the Windows XP systems in April 2014 will only add to the risk level as security vulnerabilities will no longer be addressed. In effect, this allows all individuals and organisations generating malware and/or preparing cyber-attacks to enhance their triumphs.

With the multitude of reports covering cyber security threats pointing to a rise in incidents, companies utilizing IT for critical operational purposes require better vigilance. A lack of adequate security awareness and preparedness against cyber security threats could end up becoming a major issue for a large number of companies in Belgium.

Fortunately not all is lost, but this requires awareness and organised behaviour to diminish existing cyber security risks.

*SANS Scada and Process Control Security Survey (February 2013)

Executive Summary

Loss of digital functionality, unavailability of computer systems, can, in some instances, cause direct financial impact or even grievous harm. Therefore the security threats to IT systems, and especially industrial control systems (ICS), are a growing global menace. Continued growth in digitalisation and automation will aggravate the menace as more interconnected systems become exploitable as targets. Organisations purchasing new systems will need to become more demanding on the security front from the vendors, integrators and consultants that provide and install these tools.

Of nearly 100 participants to this survey, 63 responded that their industrial control systems are crucially or very important to their organisations operations. Over half indicated that interruption or unavailability of these systems could have a disruptive impact for their organisation. Yet only a quarter of the respondents envisaged upgrades or expansion within a 5 year period. The expansive usage of Windows XP in industrial environments means that the risk to these systems will increase immediately following the demise of the OS, April 8th 2014.

This survey shows that the awareness and understanding of the cyber risk to ICS is immature in Belgium. Those companies actively pursuing risk mitigation tend to be larger multinational or global players, specialized sectors with strong adherence to quality and compliance factors, and those organisations belonging to critical infrastructure sectors (such as energy, transport, water & waste management). Medium to small companies are most at risk from cyber security threats. The impact due to disruption or hacking of ICS varied amongst the respondents. The top concerns were potential material damage, information leakage and health and safety risks. Other comments indicated loss of production time, lasting several days, to financial loss and temporary closures. Several companies also cited environmental damage as a possible impact.

The recoverability of systems following a cyber-security incident is imperative to limit losses and avoid greater harm. It is clear from the survey that more effort will be required in this area as the testing of recovery plans was very low. Furthermore, cyber-security incidents should be managed and reported so that they become a learning process. This also means reporting such incidents at a national level to the Belgian Federal Cyber Emergency Team (CERT.be), so that cyber threats and trends analysis be shared to the benefit of everyone.

The survey does shows that some companies are taking steps to set up better defences, but there is still a long way to go to create greater awareness of the problem. The fight against cyber-security threats should never be considered as a one off effort. Security mitigation is a continuous process requiring a reiterative method of attention and improvements that keep up with technology advances and perpetrator cleverness. Hopefully this survey can help give insights in the steps that need to be considered and convince more organisations to commit to cyber threat mitigation.

Survey Approach

Purpose

The survey's primary purpose is to understand the degree of maturity in Belgian enterprises with regard to cyber security risks pertaining to industrial automation and control systems.

Participants

150 Belgian based companies (multinational subsidiaries, BEL20, SMEs) that would utilize industrial automation and control systems in their operational and production environments were contacted.

The initial contact explained the purpose of the survey (identifying the awareness and maturity of cyber security awareness for industrial control systems) and was aimed at identifying the best placed individual to answer the survey questions.

The survey itself is based on the answers of 95 respondents of which 67 indicated that they utilize industrial control systems in their daily operations.

Approach

As all security type surveys can be difficult to manage due to the sensitivity of the information, it was decided that the whole survey would be conducted via phone interviews.

Content

We prepared 3 sets of questions to extract the necessary information for the survey. The first set focused on general information concerning the respondent company information, awareness of security cyber threats and the importance of industrial control systems. The second set of questions focusing on organisational (67 respondents) concerns concerning security threats to ICS. A third set of questions were prepared for committed respondents, 28 of them, willing to provide answer to security readiness measures already applied in their production environments.

Gratitude

I would like to this opportunity to thank all respondents for the time and effort they provided in supporting this survey. Without their involvement this report would not carry the necessary weight to raise awareness of the threat for all companies in Belgium.

1 Generic Survey Information

1.1 Respondents Organisation Information

The survey focused on sectors that utilize significant amounts of industrial automation in their operational and production environments.

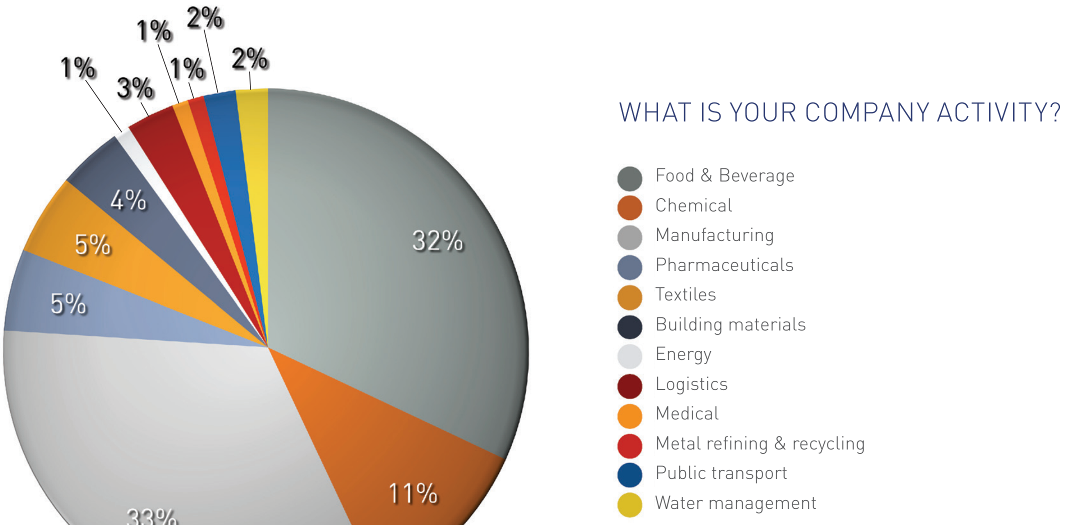


Figure 1. Company activity.

Manufacturing (32%) and food & beverage (31%) industries are best represented, but companies from several sectors took part in the survey.

Companies contacted represented a variety of organizational sizes ranging from multinationals with over 1000 employees (24%), to large and medium sized enterprises (30%) with 100 to 1000 employees, and to small enterprises (45%) with fewer than 100 employees.

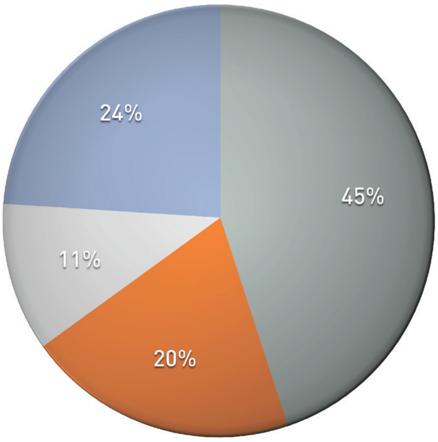


Figure 2. Company size.

1

Individual responses to the survey came from a larger diversity of roles than expected. These have been consolidated into similar type roles for analysis purposes. The largest respondent roles by far, over half, were from operations or production, followed by general management roles (owners and directors) at 15% and IT/technical/maintenance type roles (14%). Interestingly, none of the respondents identified their primary role as security.

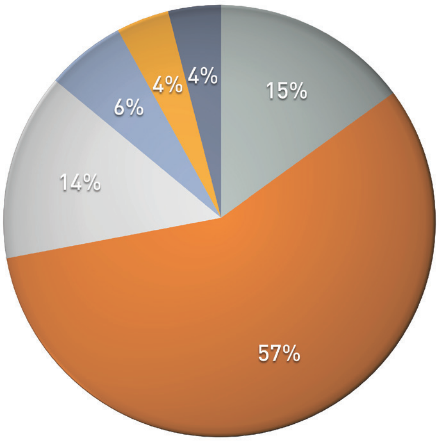


Figure 3. Respondents Roles.

1.2 Industrial Control Systems Importance in the Organisation

The degree of industrial automation for each respondent is important, as this reflects the degree of dependency the organisation places on these systems. A full 40% of respondents indicated that a large proportion of industrial systems are in use or have practically fully automated their production environments. Another 20% of the respondents' utilized automation in their production environment of which 10% indicated that their automation systems were in stand-alone mode, meaning that these systems are not networked. The remaining respondents did not utilize digitalized automation in their production environment. This points to either software or applications which are not viewed as industrial type systems (such as access control, fire detection, etc...), operational systems performing logistics or other analytic activities, or manual activities.

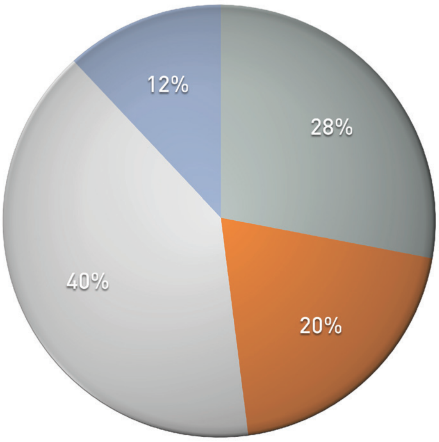
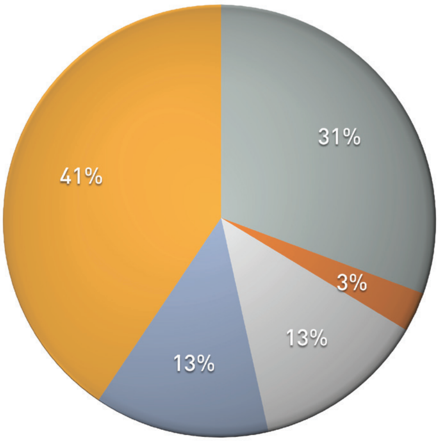


Figure 4. Industrial automation in usage.

The largest group of respondents described these systems as important (40%) to their company's daily operations. Additionally, a quarter considered that these systems were either very or moderately important to their operations. A third thought that the systems importance was either low or not important which closely reflects the number of respondents stating no automation in their production environments.

Organisations considering that the ICS was important was spread across all sections of activities and size of companies.

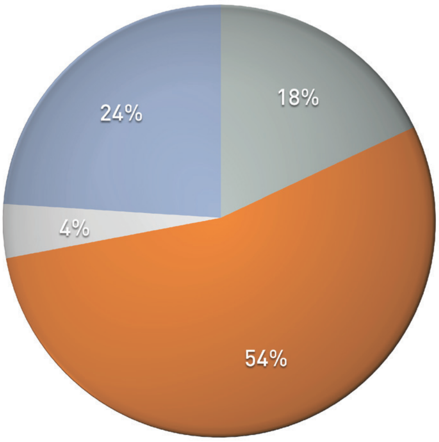


ARE/WILL THESE INDUSTRIAL CONTROL SYSTEMS BE IMPORTANT TO YOUR OPERATIONS/PRODUCTION?

Figure 5. Importance of industrial automation systems.

Over half of respondents indicated that they had no concrete plans to upgrade or expand their current automation within the next year. Only a quarter envisaged upgrades or expansion within a 5 year period. This leaves many open questions concerning how organisations will handle the security of their current systems (Windows XP).

A greater number of organizations (30%), those with under 100 employees, indicated delayed investment in future upgrades or purchases.

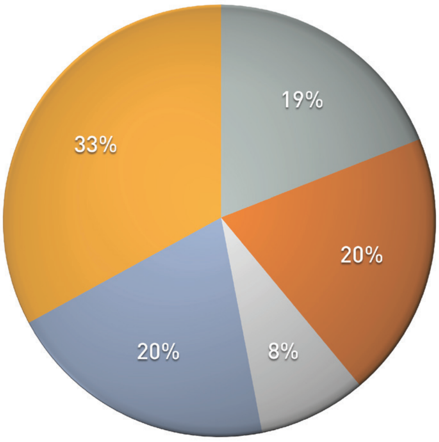


WILL YOU BE PURCHASING/ UPGRADING INDUSTRIAL CONTROL SYSTEMS IN THE FUTURE?

Figure 6. Plans for automation upgrade/increase.

1.3 Awareness of Cyber Security Risks

The awareness of security risks from the respondents was lower than expected considering the large media attention surrounding cyber security. A third of responses considered that their sector was well aware of the cyber security threat. However, 20% thought that that the awareness of IT-security in their sector was not adequate. This leaves a large degree of uncertainty concerning the awareness of cyber security threats.

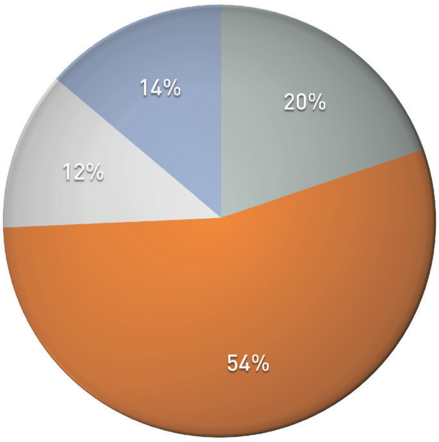


DO YOU THINK THAT COMPANIES IN YOUR INDUSTRY ARE CLEARLY AWARE OF CYBER SECURITY RISKS TO IT SYSTEMS?

Figure 7. Awareness of cyber security risks.

The awareness of cyber security threats on industrial automation systems was even more disheartening. A clear half of respondents thought that companies in their sector were unaware of such security threats. With only 10% adamant that those risks were known in their sector. Many of these tended to be multinational organizations and sectors more attuned to such threats (such as organisations identified as critical infrastructure).

It is important to note that close to half of the organizations surveyed stated that their industry was generally not aware of ICS cyber risk where from the food and beverage industry.



DO YOU THINK THAT COMPANIES IN YOUR INDUSTRY CONSIDER THAT INDUSTRIAL CONTROL SYSTEMS ARE AT RISK FROM CYBER SECURITY THREATS?

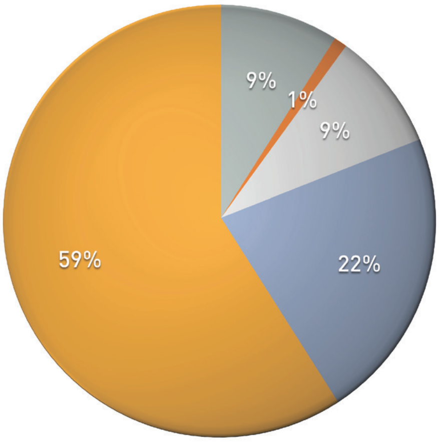
Figure 8. Awareness of cyber security risks to industrial systems.

2 Respondents Security Readiness Program for Industrial Control Systems

This section focus is on the organisational security preparedness for their ICS. The numbers utilized focused only on those respondents indicating that they were utilizing industrial control systems in their operations. As such, we have 67 respondents for this section and not the 95 as in the previous section.

When questioned about the potential impact of unavailability to industrial systems more than three quarter of the respondents indicated high to medium impact levels for their organisations. The remaining respondents either considered the impact low or were unsure.

The respondents were evenly represented across sectors and organisation size



ARE/WILL THESE INDUSTRIAL CONTROL SYSTEMS BE IMPORTANT TO YOUR OPERATIONS/PRODUCTION?

- ● No answer
- ● I don't know
- ● Low
- ● Medium
- ● High

Figure 9. Impact of unavailability of industrial systems.

Respondents were then asked to identify three concerns to their operations that could be caused by disruption to their industrial systems. All respondents showed apprehension toward material damage (to be regarded as physical damage to systems, machines, products...), information leakage, health and safety risks as their biggest worries.

The second level of concerns revolved around production loss, environmental damage or financial loss. A respondent also mentioned quality control loss as a concern but this would also be included by several respondents in the material loss category.

It goes without saying, that all disruption would inevitably include some sort of financial loss to an organisation.

HOW COULD DISRUPTIONS/HACKING TO CRITICAL INDUSTRIAL SYSTEMS AFFECT YOUR COMPANY?

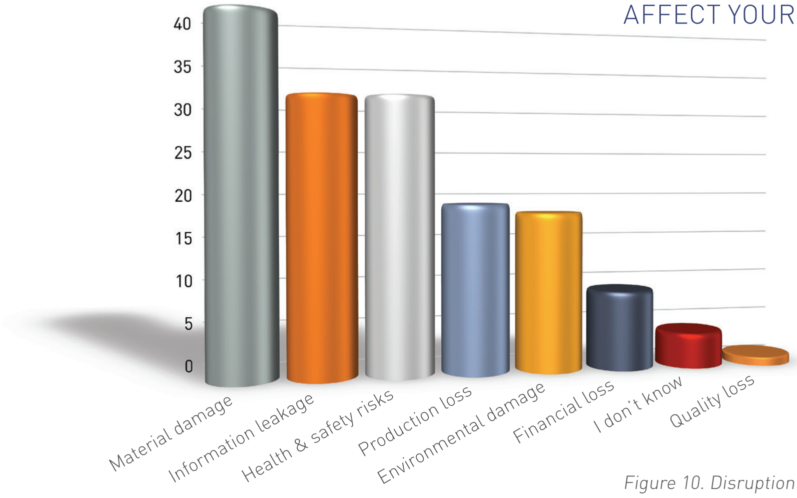
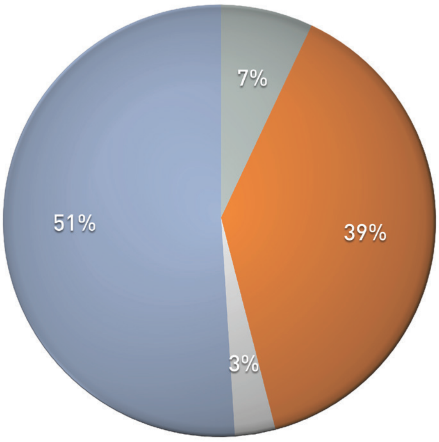


Figure 10. Disruption affect to industrial systems.

2

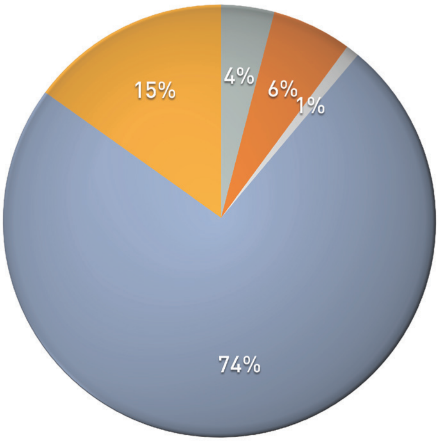
Formalized policies and procedures is an indication of a company's maturity with regards to IT security. The survey indicates that such formalization is observed by half the respondents. Of this group the formal policies came from either security requirements or quality control compliance requirements (food & beverage). A further 39% had no formalized procedures in place to deal with cyber security threats to their IT systems, including their industrial automation. This does not indicate that no security precautions were in place, some respondents indicated that actions had been taken but not in a formalized manner.



DOES YOUR COMPANY HAVE FORMALIZED POLICIES AND PROCEDURES STATING SECURITY REQUIREMENTS?

Figure 11. Formalized security policies and procedures.

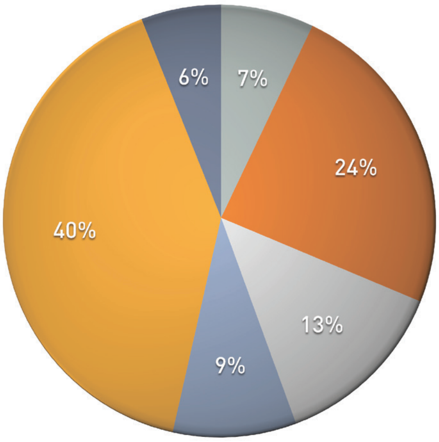
When questioned about their approach to a security vision or strategy nearly three quarters of respondents indicated that this occurred internally. The remaining respondents specified this activity was supported by external support through either their system vendors (15%) or specialist (6%). There was no indication that external support was favoured by multinational organisations nor specific sectors.



HOW DOES YOUR COMPANY BUILD A VISION OF CYBER SECURITY RISKS TO INDUSTRIAL SYSTEMS?

Figure 12. Security vision for industrial systems.

There is a positive sign when questions focused on reasons for implementing security goals within the respondent's organisation; 40% clearly advocated limiting unauthorized access, 9% following best practices and 6% were concerned with malware. However, an alarming 30% either had no answer or were unsure of the reason for their organisations security requirements.
Although compliance (13%) was also considered as a security goal, it must be clarified that compliance does not ensure protection against cyber security threats.



WHAT IS YOUR COMPANY'S PRIMARY GOAL IN SETTING UP SECURITY CONTROLS AND MEASURES FOR IT AND ICS SYSTEMS?

Figure 13. IT Security goal

The survey shows a variety of roles that are key in determining IT security measures for ICS. Over half of respondents invariably selected the IT department. The other important roles were closely linked to the protection of such systems: plant manager, technical manager or engineers. With a 4% relying on external support from vendors or consultants. The other category is a mix of different roles which is not surprising as small to medium size companies will task individuals with more than one role, generally including additional responsibility accompanying their primary role.

WHO IN YOUR ORGANIZATION IS IN CHARGE OF THE SECURITY OF YOUR INDUSTRIAL CONTROL SYSTEMS?

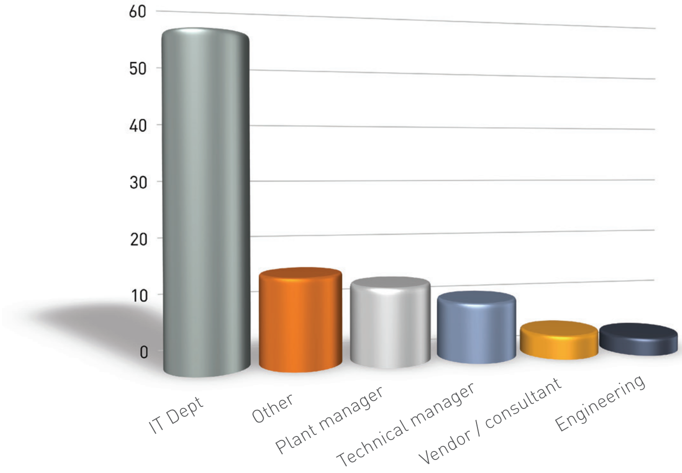
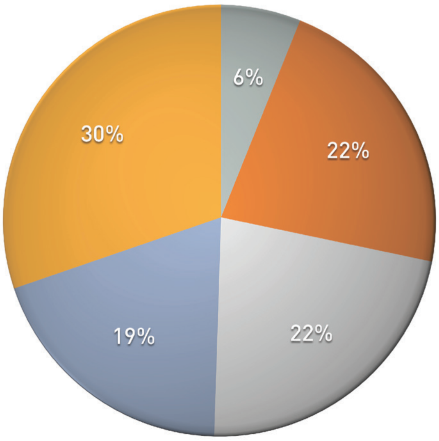


Figure 14. Security responsibility.

2

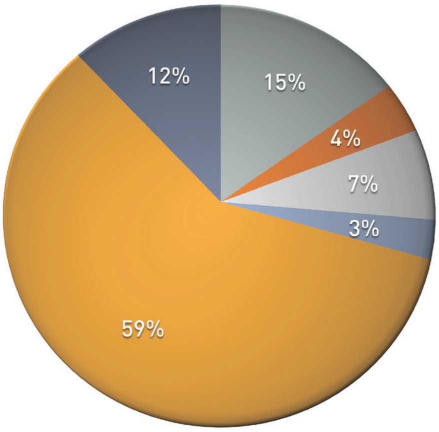
The purchase process of industrial systems did convey a concern. Almost half the respondents expressed a medium to high degree of security importance when purchasing new systems. With a fifth stating low importance and another fifth indicating not knowing if this was considered in such purchases. This adds weight to a lack of maturity in security as it is not fully integrated across all departments. A lack of security requirements at the purchasing level also indicates a potential lack of attention to security incidents liability in contractual agreements.



HOW WOULD YOU RATE THE IMPORTANCE CYBERSECURITY IN THE PURCHASE OF INDUSTRIAL CONTROL SYSTEMS?

Figure 15. Importance of security in purchasing systems.

On a final note, we inquired about the participant's disaster recovery plans in case of system failures. Upward of 70% of respondents indicated some sort of action regarding recovery of systems either through backups or machine replacements. However, only 12% of participants indicated testing of recovery plans. This is an indispensable business continuity requirement that can have negative impact in case of a severe incidents affecting system availability and information reliability.



DOES YOUR COMPANY HAVE DISASTER RECOVERY PLANS IN CASE OF A DISRUPTION TO YOUR CRITICAL INDUSTRIAL CONTROL SYSTEMS?

Figure 16. Importance of security in purchasing systems.

3 Security measures & practices for industrial systems

A third set of more technical questions were prepared for those organisations willing answer. Of the total 67 respondents with ICS 28 provide additional answers for the third section. Although these came from across all sectors a majority were from the food & beverage industry. The respondents were evenly distributed across all organisation sizes.
Instead of providing percentages for this section, an indication is given of the number respondents that answered questions related to practiced approach. Comments where then added on how to understand or improve effectiveness of vulnerability remediation.

1 How old are your current industrial control systems?

Results

The largest response group (13) indicated that their systems were between 5 and 10 years old. 6 respondents indicated their systems to be less than 5 years old, 5 respondents mentioned systems older than 15 years.

Comments

Although it is common to find industrial systems in usage for anywhere from 10 to 15 years, this is becoming a riskier practice because of the number of standard off-the-shelve machines that are being used in the production environment.
As an example, all machines based on the Windows XP operating system will be considered as obsolete systems on April 8th 2014. This does not imply that they will no longer perform their functions, it means that Microsoft will no longer provide support for these systems through security patching or services. This will in effect immediately increase the security vulnerabilities of these machines for malware and hacking.

2 Are your industrial control systems linked to corporate LAN?

Results

Of all responses, 11 indicated that there was no connectivity between the corporate IT network and the production network. However, 16 respondents indicated some degree of interconnectivity between these networks.

Comments

One of the biggest threats to industrial control systems is accessibility. This means that if a system is connected to a network than practically anyone on that network, or other interconnected networks, can gain access to the system. It is important that industrial systems be confined (limited physical and network access) and that all access to the machines is rigorously controlled.

3

3 Are the industrial control systems remotely accessible for support or maintenance?

Results

17 respondents indicated that there was some type of remote access to all or some of these systems. With 8 respondents stating that remote access to the systems was not allowed.

Comments

Remote access to systems is generally utilised for maintenance and support purposes by the system vendors. The remote access means (ADSL, modem, etc...) should be properly secured and controlled to reduce unknown security threats. If the access is not properly controlled then the organisation has allowed third party machines, and possible networks, to gain access to critical systems in their production environment. It is important to remember that third party machines and networks remain outside the control of the customer organisation and therefore require stringent remote access rules.

4 Do some ICS components or machines have access to the internet or email?

Results

Fortunately, 24 respondents indicated that internet access or email usage was not allowed on industrial control machines. Some respondents (3) did reply that such access was allowed.

Comments

The single most dangerous security risks, with regards to hacking and malware, are indeed internet access and email. It is imperative that such communication functions be removed from all industrial control systems and any other machine directly connected to the industrial network. Any machine capable of accessing the internet or emailing indicates a connection to other networks or direct access to the internet.

5 Which do you consider to be your top three security threats to your industrial controls systems?

Results

The responses to this question were in line with general security concerns: 13 responses on malware, 9 for external threats, 8 for internal threats and 9 identifying either industrial espionage or organised crime as threat concerns.

Comments

One of the biggest threats remains malware. What is interesting to know about malware is the number of forms being used to introduce it to individuals: internet clicks, email attachments, embedded in documents and pictures, etc... The perpetrators will use several means to bring the malware in to an individual but it is generally the individual that will create the infection through double clicking. Greater awareness and caution can rapidly minimize this threat.

4 Conclusion

Industrial control systems are at equal risks, if not higher in many instances, to cyber security threats than standard office environment systems. This does not mean that other critical operating systems, which are not considered as industrial systems, are any safer from the same threats. One only needs to ponder the hacker adage "if I can ping it, I can own it" to appreciate their sophistication and commitment.

All organisations have the opportunity to measure and thus recognise their cyber security risk exposure. As a first step, perform a comprehensive inventory of all digital components operated within your industrial or operational environment. The risk analysis should indicated the level of criticality and vulnerability associated to each system, taking into account networking devices and all remote access. It is only at this stage that the digital threats become understandable and manageable. All following mitigating decisions, actions and investments should than be directly attributed to minimizing identified risks.

Many organisations will be relieved to know that defences against cyber security need not always involve technology. Improvements in security processes and awareness can quickly mitigate a host of vulnerabilities. Humans still remain as the weakest link in improving security posture.

The awareness of your digital risk footprint, for whatever systems are being used, is crucial to limiting potential losses and damage to your organization. This requires a risk management approach equal to financial and operational risks; systematic analysis of risk and threats followed by mitigating actions. Cyber attacks are modern day frontline skirmishes that exempt none.

About the author

Stephen Smith is an independent advisor on digital security risks. He spent more than 25 years in the IT industry with a focus on information security and dedicated these past 5 years on risks associated with industrial control systems. A Belgian/American, he resides in Belgium and provides digital risk services to local and multinational companies in the utilities, manufacturing and transport sectors.

His effort in producing this report came from a curiosity concerning readiness of Belgian companies with regards to cyber security threats. His recent work with several companies indicated that there was a growing concern with cyber threats but that the general maturity level to deal with these threats was not ingrained in these organisations risk management culture. To this end, he commissioned a limited survey on Belgian companies, primarily those that might be utilising industrial systems, to better understand the security maturity level enabling required defences and stances to combat the growing cyber threat.

Acknowledgement

Anja Van Geert (Astraya) is independent advisor on operational risk management and strategy implementation, and partner of "Astraya Management Consulting". With more than 15 years of experience in change management and strategy alignment,.Anja has worked in many countries, for large international companies as well as smaller local organizations, showing them practical and measurable steps-by-step strategies to confidently improve their results.

For the last 5 years, she took on several interim management positions in global industrial organizations, where she focused especially on implementing Information Security, Business Continuity Management and Risk Management processes. For this report, Anja acted as the sounding board and independent reviewer of the conclusions from the survey data.

Velocitas specializes in holistic business development. Their mission 'we compel companies to grow now' show they submerge themselves in your story and support you to tackle hands-on challenges. They choose a strategic market research approach: in-depth interviews with DMU members allow them to analyse market trends. This gives them a solid basis for clear insights (target group mapping, competitors,...) and advice on market positioning and communication.

Useful Resources

Cyber Security useful sources in Belgium

- Belgian Cyber Security Guide (www.iccbelgium.be/index.php/quomodo/becybersecure)
- Federal Cyber Emergency Team (www.cert.be)

Cyber Security useful international sources

- SANS Institute (www.sans.org/critical-security-controls/)
- ENISA (www.enisa.europa.eu)
- Agence nationale de la sécurité des systèmes d'information (ANSSI) (http://www.ssi.gouv.fr)

Note

ONRIX

Stephen Smith
stephen@onrix.eu
www.onrix.eu