WHITE PAPER

Can a Solution Provider Handle Industrial Cybersecurity? 8 Questions to Ask

Felipe Sabino Costa
ISA- International Society of Automation cybersecurity instructor and Moxa LATAM Industrial Cybersecurity (IACS) Expert

MOXA®

KEY TERMS

Industrial Cybersecurity Maturity, Return on Investment (ROI), Total Cost of Ownership (TCO)

ABSTRACT

The past few years has seen an increased demand for cybersecurity in industrial applications. As a result of this, many decision makers for industrial applications are interacting with cybersecurity for the first time. While many companies hope to invest more in ramping up network security, it is essential they make informed decisions when selecting a suitable supplier or solution provider. Industrial cybersecurity is a complex topic that must include considerations about industrial operations. It is highly recommended that decision makers do not just look at the specifications shown on fact sheets or datasheets, but also consider key questions that can help ensure they choose a qualified solution provider.

This paper will provide answers to these important questions and help to guide decision makers when selecting an industrial networking solution provider for cybersecurity.

This article first appeared on the ISA Global Cybersecurity Alliance blog.

Released on October 28, 2020

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 65 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

Can a Solution Provider Handle Industrial Cybersecurity?

1. **What are the indicators that I am selecting a company that has a mature industrial cybersecurity solution?**

    There are many important factors to consider depending on the industry and application. As the literature usually does not distinguish suppliers from users, the factors mentioned below can be used as a reference for both.

    As a starting point, cybersecurity is not only a feature or product. In fact, it is a complex process that involves many different factors during different phases. It is fundamental to establish the pillars 'People', 'Processes', and 'Technologies'[1] on both sides—supplier and customer—as they pass through the life cycle including integration and maintenance of the cybersecurity solution.[2]

    While measuring the maturity of a company can be difficult, it is possible to identify some indicators that can be used to determine how mature the company is. These indicators are explored in more details in later questions and include topics such as threat intelligence processes, how quickly they respond to incidents, solutions based on solid and internationally recognized frameworks, whether the company receives vulnerability notifications from external parties, experience working on industrial applications, as well as services and support before and after purchase.[3 4 5 9 13 14 16]

2. **How do I measure the maturity of a cybersecurity solution provider?**

    It is quite difficult to define a maturity baseline for different companies that may have different frameworks and measurements. However, if we consider the ARC Cybersecurity Maturity Model, a mature company should have established a threat intelligence management process, including a full-time cybersecurity team to respond to any cyberthreats. In addition, they should be able to detect anomalies and breaches. Finally, they should also be able to anticipate potential threats instead of only responding to them, which is the most difficult to achieve.[3] This maturity model considers some key aspects, which can be good indicators of the maturity of a cybersecurity solution provider.

    In addition to the factors mentioned above, a company has a higher cybersecurity maturity level when it has implemented a solid threat intelligence process and the team effectively responds to any threats found and maps vulnerabilities.[4] Companies that are able to anticipate threats are able to offer better solutions.

    There are also some additional methodologies, such as the 'Detection Maturity Level Model – DML' and 'The Cyber Threat Intelligence Model – CTI',[5] which measure the maturity of a company based on how they handle threats (although they fall outside the scope of this paper). In order for a company to be considered mature with regards to their approach to cybersecurity, it should have established threat intelligence processes and have a dedicated team to quickly respond to any potential threats detected internally or externally.

3. Are there any independent methods to compare solutions?

Yes, inside specific industries there are some recognized frameworks such as NIST and IEC 62443, which give practical and impartial suggestions for product characteristics and general recommendations that businesses operating inside these industries should consider.[6] [7]

It is also important to consider the adoption of both vertical and horizontal standards. Horizontal standards tend to embrace a broader range of industrial applications such as ISA / IEC 62443 and vertical standards often represent a smaller sector, such as NERC CIP for the power sector.[8] Depending on the requirements of each individual sector, there may be additional vertical industry standards that can be used for reference and guidance.

Last, another important indicator to determine the maturity of a providers offering, is if they follow proven frameworks. The usage of recognized frameworks provides an independent method to compare solutions.[9]

4. How can I calculate the Return on Investment (ROI) for a cybersecurity investment?

There is still an ongoing debate about how to measure a cybersecurity investment, usually termed Return on Investment (ROI) or Return on Security Investment (ROSI). Although there is not a single agreed formula that can be easily shared,[10] it is plausible to consider the correlation between cybersecurity investments and the benefits of enhanced safety, increased production stability, and others.[11]

As cybersecurity, in a simple manner, is a combination of availability, confidentiality, and integrity (CIA triangle),[12] it is possible to infer that investments in cybersecurity directly minimize potential threats to industrial control systems and, as a consequence, increase levels of production and enhance safety. In other words, cybersecurity is the balance between the financial cost you can afford and the risk you can accept.

5. Does the solution provider receive information regarding vulnerabilities from external parties?

Another important factor to consider when evaluating a potential offering is to verify if the solution provider has an open channel to receive information about potential vulnerabilities from external parties. Being receptive to this information is fundamental to developing a more mature solution as well as increasing the reliability of the solution being offered.

For industrial control systems, this capability is still relatively new, but this openness and willingness to improve is vital to ensure they are able to provide reliable solutions.[13] Those who have already embraced this approach, are demonstrating that they are well on their way to offering a mature cybersecurity solution.

6. Does the solution provider have success stories for industrial applications that are similar to my own requirements?

The majority of the time, any given industrial application will have unique aspects. Therefore, it is important to understand if the supplier has already developed solutions for a relatively similar application. This minimizes, or at least anticipates, potential operational problems because industrial solutions differ from enterprise solutions in many respects.[14]

Whenever possible, decision makers should request a proof of concept (PoC) in order to make sure that what you are requesting can be delivered. It never hurts to emphasize, as recommended by important industrial frameworks such as NIST and ISA/IEC 62443, that any test should not be performed on a live system, but on an isolated external system first, in order to avoid disrupting live operations.[6] [13]

7. Does the solution provider have experience deploying solutions inside OT environments?

It is very important to determine whether the solution provider has enough knowledge of industrial environments so that they are able to support you. While it is true that enterprise and industrial cybersecurity solutions have a lot in common, it should not be forgotten that they are not 100% equal. In order to obtain a tailored industrial solution, different specific requirements have to be considered for each industrial application.[14]

For industrial environments, data must be passed from one device to another very quickly. For the majority of industrial applications, latency is detrimental to the system and is therefore not acceptable. In contrast to this, some latency is acceptable for the majority of enterprise applications.

The environment also plays an important role. For products being developed for industrial environments, the hardware should be built to withstand wide temperature ranges, vibration, dust, and other environmental factors. In contrast to this, an enterprise product is not normally required to go through such a rigorous testing process.[15]

Another important capability is if the software has the ability to detect and filter industrial protocols such as PROFINET, EtherNet/IP, Modbus/TCP among others, which are widely used in industrial applications.

From all of the points that have been considered, it is apparent how complex it is to implement an industrial cybersecurity solution. Thus, it is essential that the companies that are providing the cybersecurity solutions really understand this demanding sector.

8. **Will the solution provider be committed to my business?**

When selecting a solution provider, it is important to not just consider the equipment datasheets. It is important to understand whether the security solutions are connected to an overall cybersecurity strategy and how much the solution provider understands your needs.

During the past few years, there has been an increased demand and appreciation for pre- and post-sales services for the majority of cybersecurity customers.[16]

Before you purchase the solution, ensure that your solution provider is aware of your framework and that they have a good understanding of where the proposed solution fits in. The company offering the solution should act like a consultant, and be able to give you good advice for your solution. A vendor who is serious about cybersecurity needs to understand each application and suggest a specific solution for each case. The ‘one solution fits all’ model is definitely not recommended for industrial cybersecurity.

If your company does not have its own framework, a possible starting point is the Cybersecurity and Infrastructure Security Agency (CISA), which is based in the United States. It utilizes solid industrial frameworks within its Cyber Security Evaluation Tool (CSET) and uses this as a foundation to evaluate industrial control systems, including frameworks such as NIST and ISA/IEC 62443 among others.[17] As each country may have its own regulatory agency, we suggest checking your country’s agency framework recommendations if you live outside the United States.

Finally, you should list which services are available after you have purchased the solution such as warranty, troubleshooting, SLA, and others. From here, you can decide which services are more important and consider the total cost of ownership (TCO) based on the needs of your company.

Conclusion

In conclusion, it is worth remembering the following two points. The first is that there is an optimal point between the financial cost and level of protection required. Second, IT cybersecurity may not be suitable for an OT environment, so selecting an experienced industrial networking solution provider should be a requirement.

REFERENCES

1. "IEC Cyber security Brochure overview," International Electrotechnical Commission, 2018. https://www.iec.ch/cybersecurity/?ref=extfooter
2. "Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About vulnerabilities in Industrial Control Systems and Critical Infrastructure". Daniel Kapellmann, Rhyner Washburn, 2019.
3. "Cybersecurity Maturity Model," ARC, Advisory Group, 2019. https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model
4. "A survey on technical threat intelligence in the age of sophisticated cyber attacks". Wiem Tounsi, Helmi Rais, 2018
5. "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence". Vasileios Mavroeidis, Siri Bromander, 2017
6. NIST Special Publication 800-82 Revision 2
7. "IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components," International Electrotechnical Commission, 2019.
8. "Systematic cybersecurity checking approach for critical infrastructures including IEC-61850 power substation conforming ISA / IEC-62443", Felipe Sabino Costa, 2019
9. "Cybersecurity In Distribution Automation: Approach For Common Referential Leveraging Standardization". Jean-Luc BATARD, Mathieu SALLES Eric SUPTITZ, 2019
10. "Cyber KPI for Return on Security Investment". Cyril Onwubiko, Austine Onwubiko, 2019.
11. "Buenas prácticas para el diagnóstico de ciberseguridad en entornos industriales". Centro de Ciberseguridad Industrial, 2014
12. "From information security to cyber security" Rossouw von Solms, Johan van Niekerk, 2013.
13. ANSI/ISA-62443-2-4 (99.02.04), Security for industrial automation and control systems: Part 2-4, Installation and maintenance requirements for IACS suppliers
14. "SCADA System Cyber Security – A Comparison of Standards". Teodor Sommestad, Göran N. Ericsson, Jakob Nordlander. 2010
15. "Introduction to Industrial Control Networks" Brendan Galloway and Gerhard P. Hancke, 2012
16. "Critical success factors for supplier selection: an update" Cheraghi, S. H.; Dadashzadeh M.; Subramanian M.; Demantra. 2004
17. Cybersecurity and Infrastructure Security Agency (CISA) CSET 9.2.0 Release Notes",2019

Disclaimer
This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.