Key Priorities for Industrial and IIoT Cybersecurity



Global Risk Consultants®

White paper

Abstract

Modern businesses, in industries ranging from commercial aerospace and defense to manufacturing and energy, must all reckon with a wide variety of cybersecurity threats. Some of the most threatening are related to infrastructure of hardware and software that comprise organizations' Industrial 4.0 frameworks — often referred to as the industrial internet of things (IIoT). Strengthening your overall cybersecurity not only requires the implementation of advanced security solutions, but must also involve increased awareness of online threats among staff as well as the adoption of effective cybersecurity standards and practices. Data loss or theft resulting from ransomware assaults can affect organizations in areas ranging from compliance, reputation and legal liability, to the financial bottom line. Our white paper explores best practices and options for comprehensive IIoT cyber security.

Contents

ABOUT THE EXPERTS..... 2

1 INTRODUCTION..... 3

2 THE SPECTER OF RANSOMWARE..... 4

3 THE DIVERSE LANDSCAPE OF CYBERTHREATS..... 4

4 OVERCOMING KEY OBSTACLES..... 5

5 CEMENTING INDUSTRIAL CYBER SECURITY STANDARDS WITH TÜV SÜD..... 7

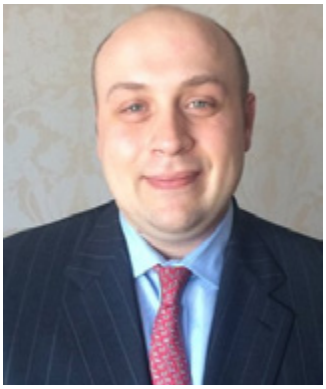
About the Experts



Andrea Blair, PE, CBCP, CBRM, CBRITP
Senior Consultant & Practice Leader - Business Continuity and Supply Chain Solutions at TÜV SÜD Global Risk Consultants
In addition to her role as Senior Consultant, Andrea Blair, PE serves as the Business Continuity and Supply Chain Solutions Practice Leader. Ms. Blair specializes in assessing client property risk trends and vulnerabilities, developing strategies to address them, and documenting these property improvements to underwriters. This process is critical in reducing property and business interruption (BI) premiums for clients. Ms. Blair possesses over 25 years of experience in a wide variety of industries and is a licensed Professional Engineer (PE), a Certified Business Continuity Professional (CBCP), a Certified Business Resilience Manager (CBRM) and a Certified Business Resilience IT Professional (CBRITP).



Craig Casillas
Digital Transformation- Industry 4.0 at TÜV SÜD America
Craig Casillas is the leader of sales in digital transformation and Industry 4.0 for TÜV SÜD America. With his 20 years of expertise with TÜV SÜD, Craig is a trusted partner of choice for any company would be lucky to have. Craig is passionate about technology and is inspired by the possibilities each individual business holds. Digital transformation is already revolutionizing every aspect of our lives, changing the way we live, work and play. Throughout this period of uncertainty, Craig is striving to add value to governments, businesses and consumers worldwide. Our aim is to inspire trust in technology, enabling progress by managing technology-related risks and facilitating change. This commitment is embodied in the new claim “Add value. Inspire trust.” United by the belief that technology should better people’s lives, we work alongside our customers to anticipate and capitalize on technological developments.



Edward Chandler
Account Executive at TÜV SÜD America

For Ed Chandler, Business Assurance for TÜV SÜD Americas comes with a digital twist. As the top person for cybersecurity needs, Ed works to help companies manage their risk landscape and minimize their exposure both to criminals and regulatory fines. Ed joined the TÜV SÜD family in June of 2018, coming with 10 years within the cyber security industry. During this time Ed has helped organizations plan, implement, and manage security and compliance initiatives from industries such as: Manufacturing, Healthcare, Financial Services, Government, and Education. Specifically, with topics such as, but not limited to: Visibility, PCI-DSS, FFIEC, GLBA, SOX, SAP, FERPA, GDPR, and TISAX.

1. Introduction

Modern businesses, in fields ranging from commercial aerospace and defense to manufacturing and energy, must all reckon with a wide variety of cybersecurity threats. Some of the most alarming are those marshaled against the combined infrastructure of hardware and software that comprise organizations' Industrial 4.0 frameworks — often referred to as the industrial internet of things (IIoT). Although research by McKinsey & Company projects that cybersecurity spending will most likely remain static or decrease among many businesses (particularly those whose bottom lines were significantly hurt by the COVID-19 pandemic),[1] it's important not to let these threat vectors fall off of the radar.



The value of Industry 4.0/IIoT system configurations is too great for facilities to ignore, but the resulting risks must be examined and reckoned with. It is not just a threat to IT operations, but they pose a significant threat to manufacturing as well. Even the briefest interruption of processes that comes with such hazards can seriously jeopardize operations. Furthermore, with dangerous malware and exploits hitting the internet on what seems like a daily basis, the interruptions such threats can cause are rarely brief.

Bolstering overall cybersecurity not only requires the implementation of advanced security solutions (endpoint detection and response platforms, anti-malware tools and more), but must also involve increased awareness of online threats among staff as well as the adoption of effective cybersecurity standards and practices. Data loss or theft resulting from ransomware assaults can affect organizations in areas ranging from compliance, reputation and legal liability, to the financial bottom line.

2. The Specter of Ransomware

According to a joint study conducted by Kaspersky Labs and ARC Advisory Group in July 2019, most businesses within the various sectors of manufacturing, heavy industry, energy and utilities cited ransomware as the greatest danger they faced.[2]

These attacks, in which malicious persons infiltrate organizations' networks through a variety of means (most often via phishing scams and other methods of social engineering) allow interlopers to seize control of systems and shut them down or steal and encrypt information. Unless ransom demands (which are about $84,000 on average in the U.S., per Emsisoft) are met, attackers will not hesitate to permanently encrypt data, destroy files, keep information technology and operational technology offline or wreak havoc in other ways. (Approximately one-third of ransomware targets ultimately pay up, as a separate Kaspersky report found,[3] and FBI analysis found that such victims surrendered more than $140 million to hackers between October 2013 and November 2019.[4])

These attacks are particularly devastating to manufacturers and aerospace firms. In one example observed by members of the TÜV SÜD team, a client in the latter field that bore the brunt of a ransomware assault ultimately had to discard its entire IT network and rebuild it from scratch.[5] This forced the wholesale shutdown of production for several weeks, jeopardizing not only the company's bottom line but also its customer relationships, partnerships and even regulatory compliance due to the sheer amount of data lost.



Did you know?

Approximately one-third of ransomware targets pay up... such victims surrendered more than

$140 million USD

to hackers between October 2013 and November 2019.



3. The Diverse Landscape of Cyberthreats

Beyond ransomware, cyberattacks of any kind that compromise major tenets of IIoT infrastructure and hosts can be just as devastating, due to their close links to industrial organizations' operational technology (OT). The connections here mean that breaking into the IIoT through just a few key devices may lead to catastrophic results, such as the shutdown of industrial control systems or even municipal utilities like electrical grids. Disturbingly, while about 80% of companies recognized the gravity of OT cyberthreats, only 31% currently had an incident response and resiliency program in place to address such dangers, with 37% saying they were planning to eventually implement one.[6]

Internal breaches are another prominent concern- not just rogue employees destroying files but also the risk of employees making unintentional yet massive mistakes that lead to data exposure and misuse. The latter, not infrequently, stems from a lack of standardized security procedures that should be cemented in formal cybersecurity policies, and often aren't.

But when push comes to shove, the simple truth is that manufacturers and industrial firms must be prepared for any and all cybersecurity eventualities such as:

- Ransomware
- Malware and virus intrusion
- Advanced, persistent threats
- Insecure supply chains
- System sabotage (internal and external, physical or otherwise)

These rank highest on the list, and IIoT arguably represents the biggest specific point of vulnerability. However, more obscure cyberthreats like botnets, SQL injections targeting database operations and unprecedented zero-day attacks should also be included in any industrial cybersecurity strategy.

4. Overcoming Key Obstacles

Organizations seeking to put new or improved cybersecurity measures in place (and properly maintain them going forward) will have to consider three essential factors above all others — people, processes and technology. A deficiency in one will often lead to issues with one or both of the others.



People: Instituting cybersecurity training (and re-training) will be essential, as it can lead to initially troubling but ultimately helpful insights regarding awareness across the workforce. For example, an audit team once offered members of an organization branded flash drives as an apparent promotional reward — drives carrying a malware strain. While ultimately harmless to devices exposed to the memory sticks because this took place under controlled conditions,[7] it illustrated how easy it can be for anyone to lose sight of cybersecurity concerns.

The end goal of exercises like this or other demonstrations IT leaders can conduct on their own is to keep staff sharp. Implementing a clear cybersecurity policy and ensuring it is adhered to will do even more.



Processes: The tenets of an organization's cybersecurity mandates should be informed by tried and true practices that have been codified within world-renowned industry standards. ISO's 27000 series can be especially useful here- specifically standards like 27001 (Information Security Management Systems), 27017 (Infosec Controls for Use with Cloud Services) and 27018 (Protection of Personally Identifiable Information), to name just a few. Within industrial sectors, it will also be important to follow the ISA/IEC 62443 standard for establishing effective cybersecurity measures within industrial control systems.[8]



Technology: Implementing or updating tools such as firewalls, anti-virus software and anti-malware tools, or replacing existing solutions with newer iterations (if relying on legacy platforms), will be essential for the maintenance of any cybersecurity strategy. Regularly conducting vulnerability assessments and penetration tests serves a similar purpose. In addition, setting up physical and cloud data backups will be key to making it through worst-case scenarios.

Connections between IT and OT, which exist in any IIoT framework, are essential for more efficient operations. Whatever risk they may entail in a vacuum is worth it for the advantages such integration brings- as long as the industrial cybersecurity strategy that safeguard them is based on a similarly integrated approach that simultaneously addresses IT and OT.[9]

Comprehensive risk assessment efforts, as well as business continuity and resiliency planning, will also play important roles in any campaign to establish a robust industrial cybersecurity framework. The former's value stems from its proactive nature: Organizations can examine trends within their industry as well as historical incidents (if any have occurred), determine the most likely risks to their IT and OT and allocate resources according to hierarchy of needs. The latter, meanwhile, ensures that a company's hope for recovery in the wake of a ransomware or malware attack extends beyond backed-up data.

5. Cementing industrial cybersecurity standards with TÜV SÜD

The biggest mistake organizations make when implementing an Industry 4.0 digital transformation initiative is going it alone. Doing so wastes time and money in all operational areas, including IIoT security.

TÜV SÜD represents an ideal partner for the creation of such a reliable industrial cybersecurity protocol and establishing a holistic approach to identifying and quantifying risk and then creating a framework to mitigate it. We offer certifications in the aforementioned ISO and IEC security standards, as well as dozens of other sets of pertinent stipulations, ranging from the EU's General Data Privacy Regulation to various guidelines from the National Institute of Standards and Technology in the U.S. TÜV SÜD GRC offers risk analysis to help pinpoint the related risk to your organization including business interruption (IBI), supplier interruption, and contingent business interruption (CBI).

Our teams also conduct assessment services per the standards of the SMART Industry Readiness Index, provide cybersecurity training exercises and resiliency consultations, conduct vulnerability scans and penetration tests and can also undertake cybersecurity audits of organizations within your supply chain.

Altogether, TÜV SÜD and TÜV SÜD GRC are trusted partners for industrial cybersecurity, aiding you with assessment and auditing and remediating flaws as necessary.



ENDNOTES

[1] McKinsey & Company. "COVID-19 crisis shifts cybersecurity priorities and budgets," McKinsey & Company. July 21, 2020.

[2] Menze, Thomas. "The State of Industrial Cybersecurity," ARC/Kaspersky. July 2019.

[3] Kaspersky. "Ransomware Revealed: Paying for the Protection of Your Privacy," Kaspersky. March 2020.

[4] Spadaforza, Anthony. "FBI: Over $140 million handed over to ransomware attackers," TechRadar. February 28, 2020.

[5] Interview with Andrea Blair, Edward Chandler and Craig Casillas of TÜV SÜD.

[5] Interview with Andrea Blair, Edward Chandler and Craig Casillas of TÜV SÜD.

[6] ARC/Kaspersky joint report.

[7] Blair/Casillas/Chandler interview.

[8] International Society of Automation, "New ISA/IEC 62443 standard specifies security capabilities for control system components." ISA.

[9] Franzetti, Davide. "Industrial Cybersecurity Needs Broad & Deep OT/IoT Threat Visibility," Security Boulevard. February 4, 2020.

COPYRIGHT NOTICE

The information contained in this document represents the current view of Global Risk Consultants Corp. on the issues discussed as of the date of publication. Because Global Risk Consultants Corp. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of TÜV SÜD America, and TÜV SÜD America cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. TÜV SÜD America makes no warranties, express, implied or statutory, as to the information in this document. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of TÜV SÜD America. TÜV SÜD America may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from TÜV SÜD America, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. ANY REPRODUCTION, ADAPTATION OR TRANSLATION OF THIS DOCUMENT WITHOUT PRIOR WRITTEN PERMISSION IS PROHIBITED, EXCEPT AS ALLOWED UNDER THE COPYRIGHT LAWS. © TÜV SÜD America – 2020 – All rights reserved.

DISCLAIMER

All reasonable measures have been taken to ensure the quality, reliability, and accuracy of the information in the content. However, TÜV SÜD America is not responsible for the third-party content contained in this publication. TÜV SÜD America makes no warranties or representations, expressed or implied, as to the accuracy or completeness of information contained in this publication. This publication is intended to provide general information on a particular subject or subjects and is not an exhaustive treatment of such subject(s). Accordingly, the information in this publication is not intended to constitute consulting or professional advice or services. If you are seeking advice on any matters relating to information in this publication, you should – where appropriate – contact us directly with your specific query or seek advice from qualified professional people. TÜV SÜD America ensures that the provision of its services meets independence, impartiality and objectivity requirements. The information contained in this publication may not be copied, quoted, or referred to in any other publication or materials without the prior written consent of TÜV SÜD America. All rights reserved © 2020 TÜV SÜD America.

America

Add value.
Inspire trust.

Global Risk Consultants®

Find out more about TÜV SÜD & TÜV SÜD GRC's IIoT solutions

https://www.tuvsud.com/en-us/digital-service/industry-40

https://www.tuvsud.com/en-us/contact-us

Choose certainty. Inspire trust.

TÜV SÜD is a premium quality, safety and sustainability solutions provider that specialises in testing, inspection, auditing, certification, training and knowledge services. Represented in over 1,000 locations worldwide, we hold accreditations in Europe, the Americas, the Middle East, Asia and Africa. By delivering objective solutions to our customers, we add tangible value to businesses, consumers and the environment.

TÜV SÜD GRC HEADQUARTERS
TÜV SÜD Global Risk Consultants
100 Walnut Ave, Suite 501
Clark, NJ 07066
+1 732 827 4400

TÜV SÜD America HEADQUARTERS
10 Centennial Drive
Peabody, MA, 01960
United States of America
+1 978 573-2500

GLOBAL HEADQUARTERS
TÜV SÜD AG
Westendstr. 199
80686 Munich Germany
+49 89 5791 0
www.tuv-sud.com