Cyber Security Month
October 2021

Cybersecurity and Data Transformation
Challenges & Best Practices

MANUFACTURING INDUSTRY

FIND YOUR BLIND SPOT

BDO

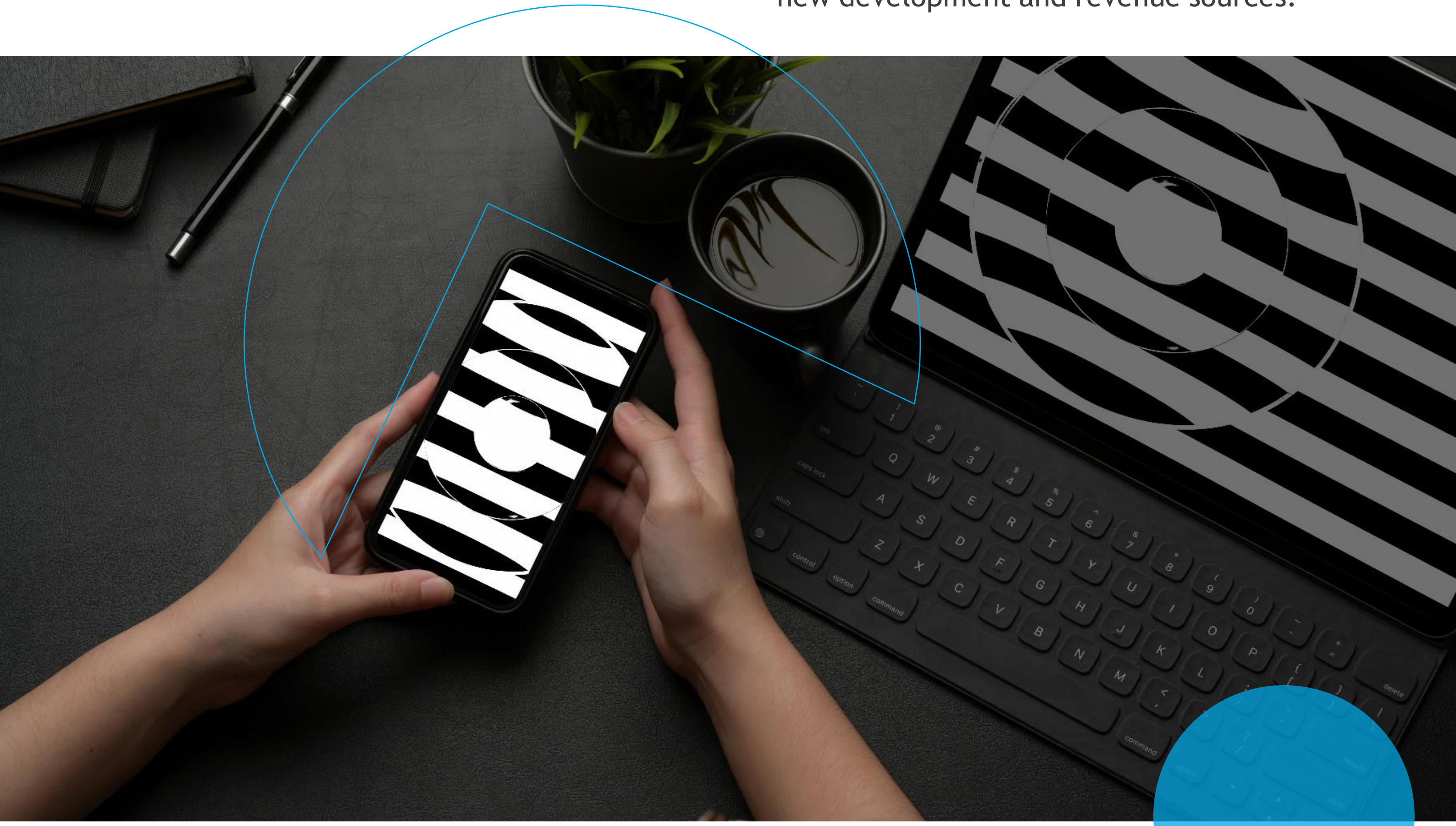
INDUSTRY 4.01

The Manufacturing Industry is overgoing a technological transformation that is changing the future of the industry. The Industry is still in its early steps of adopting digital data, digital connectivity and digital processing. Digital transformation has brought significant changes to all key areas of the manufacturing processes including performance analytics, the agility of research and development and in many cases has also brought changes into organisational structure and revenue generation streams.

In 2015, Klaus Schwab, executive chairman of the World Economic Forum has introduced the phrase "Forth Industrial Revolution" and what has been called Industry 4.0, describing the ongoing automation of traditional manufacturing and industrial practices, using smart technologies. Since then digital transformation initiatives have fostered another phrase "Smart Factory" describing modular structured factories with cyber-physical systems, decentralised monitoring, decision making and communication over and with iOT devices.[1]

The European Union Networked Information Security Agency (ENISA) defines Industry 4.0 as a "paradigm shift towards digitalised, integrated and smart value chains enabling distributed decision-making in production by incorporating new cyber-physical technologies such as IoT".[2]

Core manufacturing challenges are being successfully tackled by adopting a digital mindset, technologies, processes and changing the way people interact and work within that echo-system. Adopting new technologies has improved the levels of productivity by solving process inefficiencies, reducing costs and innovating new development and revenue sources.



[1] https://en.wikipedia.org/wiki/Foreign_Affairs

[2] https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

SMART FACTORIES

According to a recent Gartner smart manufacturing study, 84% of respondents agree that leadership understands and accepts the need to invest in smart manufacturing.[3] Early adopters in the manufacturing sector are increasingly taking advantage of the Smart Factory approach as advancements in IT present unequivocal improvements to ICS/OT systems that increase efficiency, scaling and quality, while mitigating risks of downtime, compliance, maintenance, and safety.

While adequate investment, design, and retraining in AI-based administrative and engineering control systems should improve labour conditions and expertise, firms can also analyse previously incomputable big data types collected from multiple sources, especially as strategic and operational goals require faster and more effective decision-making.

However, despite investments in self-sufficiency, according to Gartner's 2020 Smart Manufacturing Strategy and Implementation Trends Survey, 57% of manufacturing leaders say their organisation still lacks skilled workers to support digitisation plans.

That said, leaders and stakeholders need avoid strategic execution gaps to the manufacturing sector’s digitalisation process, primarily by gradually implementing better systems, utilising value chain ecosystems, partner networks, and industry consortiums, while giving late adopters who perceive moderate technological immaturity as a template to manage pilots, demonstrate ROI, and scale successes.

The Smart Factory no longer remains a luxury, but a necessity to manufacturing as smart manufacturing technologies are starting to be considered mainstream after gaining enough maturity following early overhype phases of adoption.

As such, the industry-specific network likely to come out of the Industrial Internet of Things (IIoT) should lead improvements in total production and operational capacity, while facilitating foresight needed to lead cooperation of broader industry strategic developments.

[3] https://blogs.gartner.com/power-of-the-profession-blog/strategy-and-execution-in-smart-manufacturing-must-meet-in-middle/

COVID-19 PANDEMIC

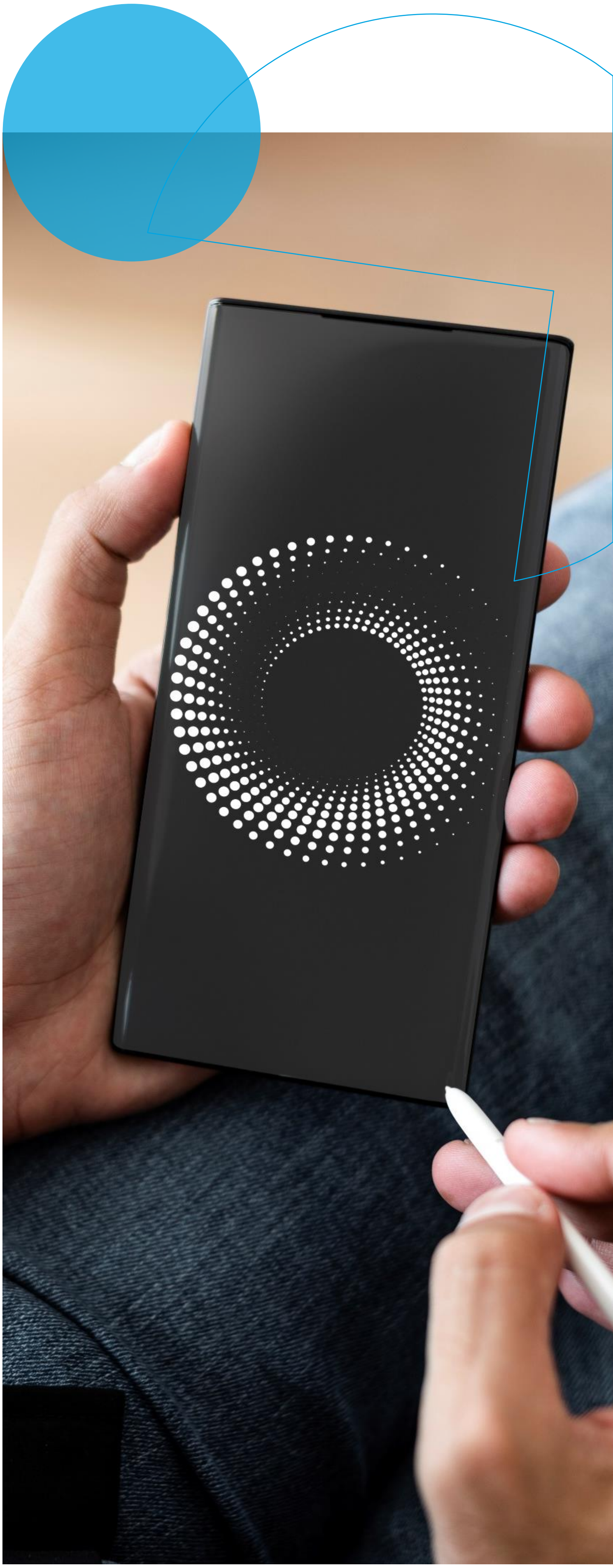
In a survey performed by Gartner, between February and March 2020, manufacturing companies reported they may face financial impact due to the pandemic and quarantine measures. Nearly half of the respondents in Gartner's survey said that they anticipated changes in operations and around 35% expected supply chain disruptions.[4] Nearly 80% of manufactures reported they expect some sort of a financial impact, 50% reported they anticipate the impact to change their operations and almost 40% reported they are facing disruption in supply chain.

The initial shock from the pandemic started to wear off during the second half of 2020; surprisingly, around 70% of the manufacturers have reported that they plan to invest, at least the same in digital enhancements of their processes as before the pandemic.

DIGITAL TRANSFORMATION

Digital Transformation in the Manufacturing Industry is expected to register a CAGR (Compound annual growth rate) of over 15% during the next four years.[5] Digital Manufacturing has helped reduce development cycles, accelerate product innovation and reduce manufacturing costs.

Digital Manufacturing is also accounted for higher revenue generation by integrating 24x7 working robotics and iOT, enabling on-demand manufacturing, operations optimization, supply chain and logistics management and product and service innovation. The emphasis on innovation in products and services has grown, where innovation will also need to handle and integrate product and asset-related information over the different stages of the product life cycle, from design to production and from sales to service and retirement.



[4] https://www.gartner.com/en/webinars/3983070/opportunities-post-covid-for-the-manufacturing-industries

[5] https://www.reportlinker.com/p05865775/Digital-Transformation-Market-in-Manufacturing-Growth-Trends-and-Forecast.html

AUTOMATION

Manufacturing is among the industries with the highest potential for automation, especially in data collection and processing, also showing significant automation potential within the manufacturing sites, supply chain and procurement.

IoT

Internet of Things (IoT) has led to new functions, services, and benefits for manufacturers. The biggest IoT use cases lie in operations, asset management, and personnel management. For example, manufacturers can establish preventative maintenance programs with real-time monitoring, improve energy efficiency and working conditions through smart air management, risk management, worker productivity, more. [6]

DIGITAL TWINS

Digital twins provide value for enterprises in three main areas. The first is in driving improvements in the manufacturing process, second is providing efficient predictive maintenance and third is developing new products based on real world usage of existing products. Digital twins can optimise an IoT deployment for maximum efficiency, as well as help designers figure out where things should go or how they operate before they are physically deployed.

MACHINE LEARNING

With the amount of data machines are collecting, it's easier than ever to utilise algorithms to quickly decide and perform the best course of action. Today's machines have proven that quality is not sacrificed by efficiency, as machines can more carefully identify and anticipate which factors will impact assembly line speed or quality.

Some examples of machine learning include, predicting waiting times, shipping times, or behaviour models for risk prevention. In addition, data generated by machines offer insights into all areas of the production process, which are integrated throughout the supply chain.

[6] https://oroinc.com/b2b-ecommerce/blog/digital-transformation-in-manufacturing

B2B-COMMERCE

Aside from delivering the right product data to customers, B2B eCommerce platforms can automatically sync data with the ERP (Enterprise Resource Planning) and WMS (Warehouse Management System) to cut down on inventory management efforts and the probability of human error. More importantly, B2B eCommerce systems allow manufacturers more flexibility in selling direct-to-customer or B2B2C without disrupting their existing channels.

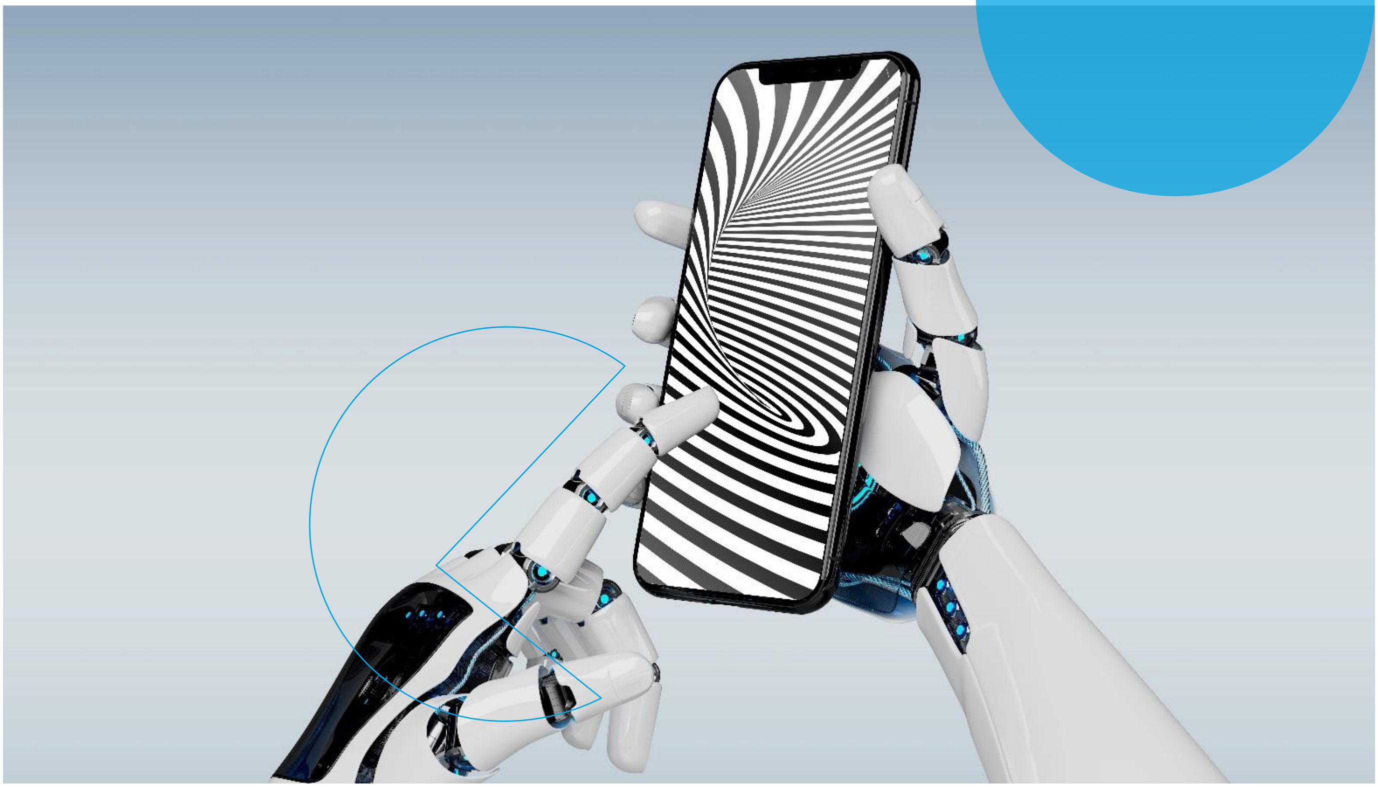
ARTIFICIAL INTELLIGENCE (AI)

As the adoption of robotics in manufacturing increases and the number of connected devices, how they interact with each other, and the volume of data are all expected to increase, AI will play a major part in giving robots more responsibility to make decisions that can further optimise processes based on real-time data collected from the production floor. Robots will also have learning capabilities from previous behavior and use of pattern recognition for decision making with better results.

ROBOTS

In a survey performed by Gartner, between February and March 2020, manufacturing companies reported they may face financial impact due to the pandemic and quarantine measures. Nearly half of the respondents in Gartner's survey said that they anticipated changes in operations and around 35% expected supply chain disruptions.4 Nearly 80% of manufactures reported they expect some sort of a financial impact, 50% reported they anticipate the impact to change their operations and almost 40% reported they are facing disruption in supply chain.

The initial shock from the pandemic started to wear off during the second half of 2020; surprisingly, around 70% of the manufacturers have reported that they plan to invest, at least the same in digital enhancements of their processes as before the pandemic.



CYBER SECURITY

The move toward Industry 4.0 has a significant impact on the connectivity of the manufacturing network. Previously isolated and running its own protocols, the manufacturing network is being slowly integrated with the IT network for real-time visibility, control and integration into various systems that make up the production line, supply chain, sales, and enterprise systems. Computers and controllers in the manufacturing network are now exposed to a wider range of threats, which require both IT administrators and OT engineers to work together to bring the security and protection of such systems up to speed without compromising any operational requirements.

A report about Cyber-Security and Manufacturing, publish by Make-UK, has put the Manufacturing Industry as the fifth most cyber-attacked sector in 2019, also describing the industrial businesses as the least protected in the UK.

The UK being one of the world's biggest manufacturing nations, with over three million people working in the industry and delivering almost half of all the UK export, make those statistics a global concern.[7] The report published more worryingly numbers as 60% of manufacturers claimed they have at some time been subject to cyber security incident, and almost a third of them said they suffered from a direct financial loss or disruption to the business as result.

"Manufactures often report over confidence in their cyber security posture leaving themselves highly exposed due to a lack of a comprehensive strategy", the report concluded. This perception has permeated into their businesses and created a barrier; preventing the roll out of comprehensive mitigation strategies.

27% of manufacturers reported they do not have a risk register or mitigation plan to limit the threat, 33% reported they do not provide awareness briefs or formal training to their employees, 41% reported they do not have a nominated lead for cyber security at board level, 49% reported they do not monitor cyber security performance through key business performance indicators, and 55% reported they do not have insurance to cover loss due to cyber-attack.

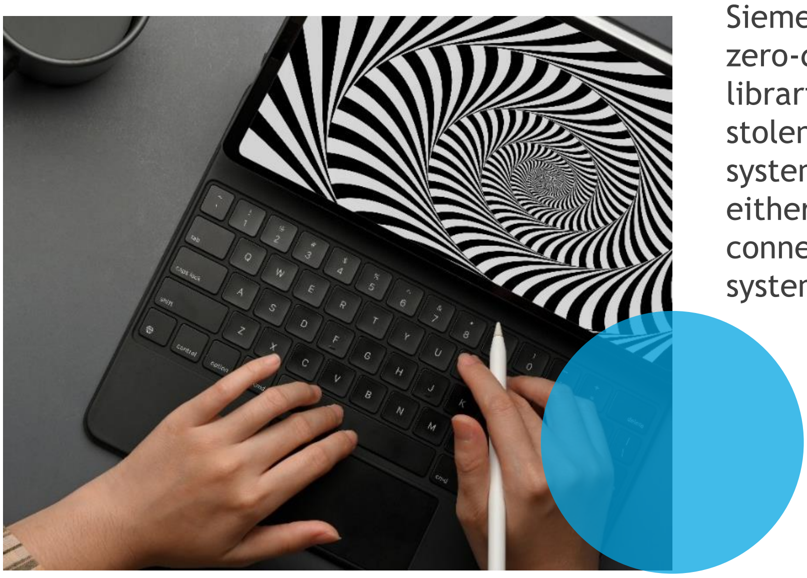
Modern manufacturing equipment has human-machine interfaces (HMIs) that allow operators and engineers to monitor and control the equipment. Programmable logic controllers (PLCs) are used to program logic into several pieces of equipment, enabling them to act based on certain conditions or thresholds as reported by other pieces of equipment or sensors. Furthermore, there are industrial grade routers, hubs, and gateways that handle the networking in the manufacturing network. Just like any normal system, these pieces of equipment and devices have vulnerabilities.

[7] https://www.makeuk.org/insights/publications/cyber-security-and-manufacturing

According to the vulnerability reports submitted to the Industrial Control Systems Computer Emergency Response Team (ICS-CERT), showed a significant jump in the number of vulnerabilities affecting manufacturing-related equipment, also showing that most of the publicly available exploits involved HMI vulnerabilities. Where HMIs are in fact applications, sometimes having web interfaces and are subjected to traditional web exploits.

According to a study by Trend Micro’s, common security problems with HMIs involve memory corruption, buffer overflows, read/write vulnerabilities, poor credential management (use of hard-coded passwords, storing passwords in recoverable format, and insufficiently protected credentials), lack of authentication and unsecure defaults clear text transmission, missing encryption and unsafe ActiveX controls.[8]

Trend Micro and Politecnico di Milano, the largest technical university in Italy, have published a research named "Vulnerable and Malicious Code in Industrial Programming". The report outlined how advanced hackers could exploit vulnerabilities in Internet-connected industrial robots and automated machines to disrupt production lines and steal intellectual property. [9]



The report also highlights how the industrial automation may not be in a position to detect and prevent such exploitation from occurring. The report is pointing out to legacy technologies, which are intrinsically difficult to replace and have not been discussed and examined from a cybersecurity perspective. The report has also demonstrated the exploitation of design flows and vulnerabilities in automation logic platforms and legacy programming languages, that enabled attackers to steal data from a robot, alter robot's movement via the network, inject dynamic malware and remote execute the code without being detected. In summary, they were able to execute a successful attack by creating a self-propagating malware, written in automation logic platforms based on proprietary, legacy programming languages.

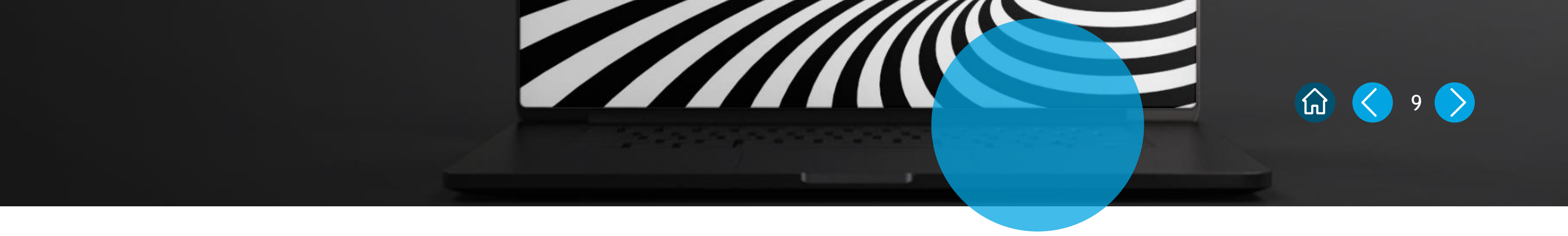
Stuxnet, is often referenced in this regard because it was the first malware that demonstrated the possibility of concealment using legacy programming languages. In 2010, Stuxnet caused a shift in focus for ICS security by demonstrating practical exploitation of the control logic in those industrial control systems.[10]

Stuxnet was a sophisticated worm-able malware designed to target only a specific Siemens ICS system. It made use of multiple zero-day vulnerabilities, modified system libraries, run an RPC server and installed stolen signed drivers on windows operating systems. It was also able to update itself either from the local network or by connecting to a command and control system and send information of its progress.

[8] https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities

[9] https://documents.trendmicro.com/assets/white_papers/wp-rogue-automation-vulnerable-and-malicious-code-in-industrial-programming.pdf

[10] https://arxiv.org/pdf/1702.05241.pdf



Another piece of malware of note is Triton, which showed that control-process-specific and device-specific malware was feasible and could have disastrous consequences.[11] Triton was the first malware designed to attack safety systems, ever seen in the wild.

Triton, was first discovered in 2017 in a petrochemical plant in the Middle East, designed to manipulate Schneider Electric's Triconex Safety Instrumented System (SIS) controllers responsible for emergency shutdown systems. Triton was built with a number of features, including the ability to read and write programs, read and write individual functions and query the state of the SIS controller.

The malware contained the capability to communicate with SIS controllers (e.g. send specific commands such as halt or read its memory content) and remotely reprogram them with an attacker-defined payload.[12] Triton was designed to shut-down manufacture plant's safety instrumented systems, which was the first-time malicious code has been deliberately written and used to put lives at risk.

Cyber-security risks to the manufacturing industries, have won global attention in parallel to the advancements in digital transformation. On May 11, 2017, President Trump signed Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. EO 13800 specifically called for a review of "the sufficiency of existing Federal policies and practices to promote appropriate market transparency of cybersecurity risk management practices by critical infrastructure entities".[13]

On April 30, 2019, the DHS released a list of 'national critical functions' that the Department and the White House views as "The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof".

On May 15, 2019, the White House released Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, saying that "The national and homeland security community was concerned about aggregated risk that comes from the use of common ICT and services".

On June 8-9, 2019 in the G20 ministerial meeting focusing on trade and the digital economy, the Ministerial Statement clearly articulated the benefits and risks that a digital world brings to industries like manufacturing, stating: "Security in a digital economy is essential for strengthening public confidence in digital technologies and the entire digital economy". The Ministerial Statement also cited the benefits and the risks stating "Manufacturing, which is one of the most crucial industries in the global economy, is becoming more digitalised, networked and intelligent", and acknowledged the risk that also comes from the that world of emerging technologies and the IoT.

[11] https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware

[12] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[13] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

CHALLENGES

On May the 20th, 2019 the European Union Agency for Cyber Security (ENISA) have published a paper which identifies the main challenges to the adoption of the security measures and security of Industry 4.0 and Industrial IoT. The ENISA study focused on addressing the security challenges related to the evolution of industrial systems and services precipitated by the introduction of Smart Manufacturing. ENISA has associated cyber-security challenges with one of the following categories: People, Processes and Technologies.

CATEGORY	CHALLENGE	DESCRIPTION
People	Lack of information security expertise	People usually only have knowledge of either IT or OT security, while Smart Manufacturing requires expertise over several areas, e.g. network security, embedded systems, OT and IT.
People	Lack of training and awareness	Manufacturing companies often are lagging in training employees who work with OT equipment and instead employ security solutions without first ensuring take-up by employees.
People	Lack of appropriate governance structure	Defined security programmes are rarely in place and in general, comprehensive programmes that consider cyber-security are lacking. It is also often noted that security related roles and responsibilities of employees are not clearly defined.
People	Lack of funding and commitment from top level management	Due consideration to cybersecurity is given 'after affect', only when a security breach directly leads to financial losses.
Processes	Liability is poorly defined	Large number of stakeholders are involved in the supply chain and in the lifecycle of Industry 4.0, therefore apportioning liability in the aftermath of a security incident becomes challenging.
Processes	Complexity of the Supply Chain	Shared ownership of connected, Industry 4.0 solutions, unclear or unspecified role assignments and lack of provisions in procurement contracts and service level agreements further complicate the issue of liability.
Processes	Lack of technical security standards	Comprehensive initiatives to address industry 4.0 and Smart Manufacturing security in a holistic manner are lagging behind.

CATEGORY	CHALLENGE	DESCRIPTION
Processes	Fragmentation of technical standards	The lack of uniform standardisation efforts at a global level results in a situation where sites that belong to one organization cannot collaborate and share expertise and solutions with each other.
Processes	Supply chain management complexity	Smart Manufacturing introduced new capabilities (End-to-End visibility, predictive analysis, automation and data-driven decision-making) that have an additional impact on the supply chain, increased inter-dependence of supply chains results in broader impact.
Processes	Scalability for supply-chain risk management	Companies need to make numerous decisions (e.g. select vendors, agree on methods of collaboration, establish organisational processes), on which the security of the final product will depend. This involves large number of people, organisations, processes and risks that need to be managed.
Technology	Legacy Systems out of support	For industrial environments, securing interconnectivity between diverse devices is often challenging, especially when considering devices that are long out of support.
Technology	Proprietary Protocols	Ensuring interoperability between devices and platforms from different vendors, is not always be possible especially then proprietary protocols are not always secure.
Technology	Different Application frameworks	Ensuring a unifying common cybersecurity baseline of security layers across all these elements: platforms, devices, protocols and frameworks, is not always possible.
Technology	Limitations in implementing security by design	Limited processing capabilities and the need to ensure long time of operation while maintaining a competitive price, affect the implementation of security features in the design phase.
Technology	Limitations in implementing fundamental protection	Patching and software updates in most cases are very hard, sometimes impossible to implement, when it comes to low-end devices.
Technology	Lack of advanced security measures	Implementation of encryption or authentication, as appose to only securing the network and leaving the devices vulnerable to attacks, sometimes are not supported.

Interconnectivity throughout manufacturing industry is characterised by an interesting mixture of OT (the industrial network), IT (the enterprise network), and IP (intellectual property). It is the only industry to combine all three, thereby creating these unique sets of challenges.

BEST PRACTICES

ENISA have published some high-level recommendations to promote cybersecurity in the manufacturing industry. [14]

CROSS-FUNCTIONAL KNOWLEDGE ON IT AND OT SECURITY

Raising awareness on basic industrial control security as well as on the secure way for transitioning to Industry 4.0 and Smart manufacturing.

Persons in charge of security within Industry 4.0 organisations should go through dedicated cybersecurity trainings that cover all necessary aspects specific to IT/OT convergence and Smart manufacturing.

INCENTIVES FOR INDUSTRY 4.0 SECURITY

Cybersecurity can be an important competitive advantage for businesses, since it leads to having secure, reliable and trustworthy products and services.

It is important to establish administrative structures for top-level management to discuss and exchange views with cybersecurity experts and CISOs and launch funding schemes to support their transition to a secure Industry 4.0 ecosystem.

BASELINE STANDARDS DEDICATED TO INDUSTRY Industry 4.0 SECURITY

Explore initiatives and guidelines that map security standards from many different sources to provide a complete point of reference and thus ensure all necessary security controls are considered. Develop

SECURE SUPPLY CHAIN MANAGEMENT PROCESSES

Conduct risk assessment at periodic intervals to identify potential Industry 4.0 supply chain risks, also considering cyber threat intelligence to monitor ongoing and emerging threat landscape. Rely on suppliers whose products comply with recognised security standards and certification schemes and follow secure software development lifecycle for Industry 4.0 products and services.

BASELINES FOR SECURITY INTEROPERABILITY

Identifying baseline security recommendations for Industry 4.0 components, services and processes based on risk analysis is a first step to approach a solution to the challenging technical constraints of this domain.

[14] https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

IN CONCLUSION

Manufacturing contributes 16% of the global Gross Domestic Product (GDP), 64% of global R&D spending, and is a leading indicator of global economic health. Embracing new transformation models that bring together technology, people, policies and processes together with making cyber-security the highest priority, is a global multinational purpose.

OPHIR ZILBIGER

Global Cyber Leader
Partner, Head of Cybersecurity Center
BDO Israel
OphirZ@bdo.co.il

NOAM HENDRUKER

Partner
Head of Cyber Consulting Group
BDO Cybersecurity Center, Israel
NoamH@bdo.co.il

TOMMY BABEL

Director
Head Threat Operations & Offensive Security
BDO Cybersecurity Center, Israel
TommyB@bdo.co.il

ROTEM BAR

Manager
Industrial Defense Division
BDO Cybersecurity Center, Israel
RotemB@bdo.co.il

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication. No entity of the BDO network, its partners, employees and agents accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any
decision based on it.

'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities. The BDO network (referred to as the 'BDO network') is an international network of independent public accounting, tax and advisory firms which are members of BDO International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited, Brussels Worldwide Services BV and the BDO member firms is a separate legal entity and has no liability for another entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the BDO member firms. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.

www.bdo.global