Keeping the lines moving:

WHY CYBERSECURITY IS CRITICAL FOR MANUFACTURING

subrosa

THE WAVE OF DIGITALIZATION IN MANUFACTURING

The digital era has ushered in massive changes in the manufacturing industry.As an industry that focuses on scalability and efficiency, it has embraced technology with open arms. Today's fast-paced market environment demands manufacturers to not only keep up with the pace of developments but also to innovate and think ahead.

Automation, IoT, smart equipment have all helped improve every facet of the manufacturing process. Be it increasing production capacities or ensuring better quality control. Interconnected control systems, automated monitoring systems, smart machinery, and real-time data analysis processes are enabling manufacturing lines to work with smooth cohesion and utmost efficiency.

Manufacturing companies must face the cyber threat head on.

HOW THIS IMPLEMENTATION OPENS UP CYBERSECURITY RISKS.

Yes, technology is an enabler on a scale never seen before. But with the immense importance that it holds, protecting these business-critical systems is a paramount need.

CYBER ATTACKS PRESENT AN IMMENSE THREAT TO INTERCONNECTED INFRASTRUCTURE

Every piece of connected technology presents a potential attack vector. Cyber threats can expose a company's infrastructure, intellectual property, finances, sensitive data, and other assets to grave threats. Digitalization and interconnectedness have led to all these business-critical systems being centralized which increases the vulnerability manifold.

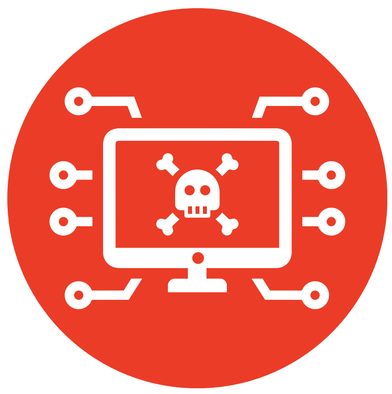
With the adoption of technology in manufacturing, the lines between different phases of manufacturing are gradually fading away. Manufacturing lines and supply chains rely on the smooth functioning of each phase. Targeted or not, even a single cyberattack may have deep implications as it can not only cripple operations at the affected point but may cause a far-reaching domino effect.

For manufacturing companies, OT infrastructure is the backbone of the company. Control units, machinery, monitoring systems are all usually controlled by a central network. Many manufacturing companies will employ cybersecurity for their IT infrastructure but leave their OT infrastructure exposed. This leaves OT infrastructure vulnerable to cyber threats. Moreover, OT infrastructure may contain components of a wide variety and legacy systems which makes cybersecurity implementation a challenge.

THE DYNAMIC LANDSCAPE AND THE ALLURE OF MANUFACTURING COMPANIES

In today’s ever-changing cyber landscape. Threats continue to emerge every day. Hackers continue to develop newer techniques and deploy more dangerous tools to exploit vulnerabilities. Cybersecurity can no longer be thought of as a mere afterthought.

Incidents like the attacks on Stuxnet in Iran and Triton in Saudi-Arabia have cemented the importance of cybersecurity for industrial networks. Attacks on critical infrastructure have shown how cybercriminals have exposed the vulnerabilities of industrial networks with increasingly sophisticated tools and techniques. Due to the value that these networks hold, manufacturing companies have become an appealing target for cyber attacks.



32% OF MSPs

report manufacturing and construction as being most target by ransomware.

of industrial companies rank cybersecurity as a top priority.

PROTECTING YOUR ASSETS

THE STATISTICS THAT TELL

The 2019 Deloitte and MAPI Smart Factory Study revealed several risks relative to smart factory initiatives, from operational to financial and strategic to compliance. Forty-eight percent of manufacturers surveyed identified operational risks, which include cybersecurity, as the greatest danger to smart factory initiatives.

IOT DEVICE WEAKNESSES

According to research by Irdeto, eight in ten companies have experienced a cyberattack on their IoT devices in the past year.

OPERATIONAL IMPACT

90% of these organizations experienced an impact affecting their operations or data as a result of the cyberattack.

MONETARY LOSS

Irdeto Global Connected Industries found that organizations in manufacturing suffered substantial losses due to IoT-related vulnerabilities, of more than $330,000 on average.

RANSOMWARE

According to a study by Kivu Consulting, the manufacturing industry spent more than any other sector (in 2019) on ransomware payments, paying out $6.9 mn.

Research conducted by IBM's X-Force IRIS incident response team revealed that 50% of organizations affected by cyber-attacks in 2019 are in the manufacturing sector. According to the same report, 60% of manufacturing firms were hit with at least one WannaCry-related attack in the first six months of 2019.

50% of organizations affected by cyber-attacks in 2019 were in the manufacturing sector.

CYBER-ATTACKS IN MANUFACTURING

NORSK HYDRO CYBER ATTACK

In March 2019, a cyber attack hit Norwegian aluminum giant Norsk Hydro. The company's operations in 40 countries and 35,000 Norsk Hydro employees were affected. The company was hit by the LockerGoga ransomware. The financial cost of the attack was estimated to be $71 million dollars.

OXO INTERNATIONAL PAYMENT SKIMMING

In 2018, OXO International discovered a vulnerability in the form of malicious code on its website. The malicious code was intended to steal customer data. OXO's customer and payment details were skimmed to a remote server by the cybercriminals.

MONDELEZ MALWARE

In June 2017, a global malware attack on Mondelez. Mondelez, one of the world's largest snack companies, was severely affected. The estimated losses due to the attack were estimated to be in excess of $100 million dollars.

DUPONT INSIDER ATTACK

In 2007, an insider attack on DuPont resulted in IP data worth hundreds of millions of dollars being stolen. The research chemist responsible for the incident had accessed over 16,000 documents. The data included DuPont's sensitive R&D material.

TOP DOWN RISK MANAGEMENT

Leadership Oversight

50% of manufacturing executives **feel they are underprotected.**

48%

of manufacturing companies lack sufficient funding

Organizaitonal Oversight

40% of the top threats **involve employees**

75% **Lack skilled talent**

Protect

Implement strategies to proactively manage cyber risk across the enterprise.

Enterprise Systems

36%

of manufacturers are most concerned with IP theft

IoT and Connected Devices

45%

use IoT devices and smart products

55%

encrypt the data on said devices

Industrial Control Systems

50%

Isolate ICS on their network

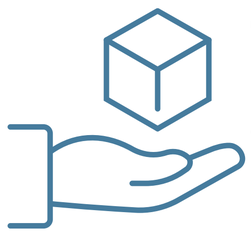
31%

Do not conduct ICS assessments

Prevent

Implement detection technologies and conduct routine technical assessments enterprise-wide.

A major concern of IT and security executives is the **frequency and sophistication of manufacturer-target cyber attack**s



77%

Perform product assessments

50%

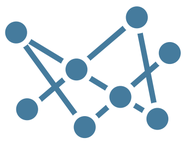
Perform ICS vulnerability assessments less than monthly

Respond

Implement plans and procedures to ensure that when an incident occurs, organizational resources can respond efficiently and in a timely manner.

37% Have had a breach within the last 12 months.

Had losses of **$1m-$10m** **38%**



37%

Have not included ICS in their incident response plans.

27%

Have not included ICS in their incident response plans.

THE DEBILITATING FALLOUT OF CYBERATTACKS

THE FINANCIAL BRUNT OF A CYBER ATTACK CAN BE IMMENSE

In some cases, cyber-attacks have permanently crippled a company's operations and in many cases, they have had to bear damages in tens of millions of dollars. It goes without saying that financial losses resulting from breaches and attacks can be sizable. The operational downtime may further jeopardize a company's finances, its obligations to clients, and its reputation. A cyberattack that results in the loss of IP could lead to the company losing its critical edge in the market. Attacks intended for corporate espionage may give access to highly-sensitive data to a competitor. Damage to critical equipment can cause a meltdown in the entire production or supply chain.

In several cases, when customers' private data is left exposed. The impact on the company's trust and reputation can be incredibly damaging. In some cases, the legal ramifications can be dire and may even stretch up to regulatory sanctions. What happens when production lines are brought to a complete standstill in a matter of minutes? What happens when an entire supply chain is crippled? What happens when a company's customers' data is exposed?In the hyper-connected and globalized business environment of today, technology plays an irreplaceable role.

In manufacturing, technology and digitalization have brought incredible changes. But, they have not made it invulnerable. Cyberattacks can devastatingly damage the entire infrastructure upon which today's companies rely on. To protect these business-critical systems and infrastructure is the need of the hour.

Cyberattacks can devastatingly damage the entire infrastructure upon which today's manufacturing companies rely on.

Our Company

We deliver cutting edge security technology solutions and services to our Clients so that they are prepared to tackle the ever growing cyber threat. Through the SubRosa Unified Risk Platform, we deliver threat intelligence, security controls validation and incident alerting and response. We employ and partner with some of the leading risk and security experts in the industry, enabling us to deliver effective services and software solutions to our clients of all sizes, across the globe.

More resources available at: https://subrosacyber.com

SUBROSA
2000 Auburn Dr
Ste 200 #366
Beachwood OH
44122
888.893.1983
info@subrosacyber.com

Since 2017 SubRosa proudly delivers cyber risk advisory and related services to public, private and government clients.

This brochure is to be used as a reference for general information only, and no content contained herein is designed to provide cyber risk professional advice or services.