ThreatQ for Manufacturing Companies

The manufacturing industry comprises various components, including raw material sourcing, production processes, quality control, and distribution. It involves machinery, skilled labor, technology, and supply chains to transform raw materials into finished goods. This sector encompasses diverse industries like automotive, electronics, textiles, and more, contributing significantly to economic growth globally.

The manufacturing industry faces a variety of challenges and concerns that can impact its overall performance and sustainability including but not limited to:

Supply Chain Disruptions: Events such as natural disasters, geopolitical issues, and pandemics can disrupt the global supply chain, affecting the timely delivery of raw materials and components.

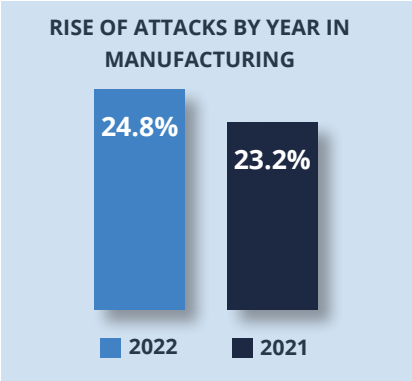
Technology Adoption and Integration: Keeping up with rapidly evolving technologies such as automation, artificial intelligence, and Industry 4.0 can be a significant challenge. Manufacturers need to invest in and integrate these technologies to stay competitive.

Cybersecurity Threats: As manufacturing processes become more connected through the Internet of Things (IoT) and other digital technologies, the industry becomes more vulnerable to cyber threats. Protecting sensitive data and ensuring the security of interconnected systems is crucial.

Cost Management: Managing production costs is a perpetual concern. This includes costs related to raw materials, energy, labor, and operational efficiency.

KEY CHALLENGES

Manufacturers need to address these concerns strategically to navigate the dynamic landscape of the industry successfully. Implementing robust risk management, investing in technology and innovation, and fostering a skilled and adaptable workforce are key components of staying competitive in the manufacturing sector.



Source: IBM Security X-Force Threat Intelligence Index 2023[1]

According to Statista, during 2022 manufacturing companies encountered nearly

25% **of the total cyber attacks.**

Source: Statista[2]

SUPPLY CHAIN DISRUPTION

Supply chain attacks are employed by cybercriminals to manipulate a company's manufacturing processes through interference with both hardware and software. Malicious software may be inserted at any point in the supply chain, potentially leading to disruptions or outages in the organization's services as a result of this cyber attack.

Source: Dragos[3]

RANSOMWARE

"The manufacturing industry suffered at least 437 ransomware attacks in 2022, making up more than 70% of these types of costly and disruptive assaults that industrial companies faced last year, according to the cybersecurity firm Dragos[3]."

One challenge encountered by manufacturing facilities is the frequent lack of visibility for operators into their systems, coupled with the use of shared credentials across information networks and operational technology systems.

OUTDATED TECHNOLOGY

Using outdated technology increases the risk of security breaches due to the absence of the latest security features. Such systems are frequently unsupported by their original developers, leaving them without essential security patches and updates. As cybercriminals continually discover new ways to access information, relying on outdated technology not only jeopardizes your data but may also result in additional expenses, either through paying criminals or losing customers. Therefore, while opting for older technology may seem like a cost-saving measure, it could ultimately expose you to significant risks and financial consequences.

Source: Infosec[4]

PHISHING SCAMS

Extensive phishing campaigns enable the perpetrators to gather various forms of sensitive information, including but not limited to bank account details, social security numbers, and credit/debit card information. Alternatively, they may coerce the victim into making a payment directly into the attacker's bank accounts. Moreover, phishing activities can be motivated by other objectives, such as acquiring sensitive data to tarnish the reputation of the targeted entity or disseminating malicious software to wreak havoc on the company's physical assets and equipment.

"According to NNT Security report, 58% of malware in the manufacturing industry is spread through web-based downloads, and it varied between Trojans and droppers in the second quarter of 2017. Reconnaissance, which includes methods of collecting vulnerabilities about the victim's computer once accessed by the hacker, represented 33% of cyber-attacks targeting the sector." Infosec[4]

Source: Blackberry[5]

HOW MUCH DAMAGE IS CAUSED

"New research out of Britain, by Make UK The Manufacturers' Organization and BlackBerry, finds that 42% of the country's manufacturers were cybercrime victims during the last 12 months. And even more unsettling is that one quarter (26%) report suffering "substantial financial loss" as the result of an attack, with losses ranging from $62,000 to $310,000 (£50,000 to £250,000).

Of those hit by a successful cyberattack, 65% report work stoppages. In that

situation, the losses instantly begin to mount. The research also reveals that 43% of organizations report that the attack against their organization caused reputational damage, which can impact both current relationships and future sales." Blackberry[5]

CREATING A LEADING DATA-DRIVEN SECURITY OPERATIONS

Serving as the hub of intelligence operations for many industries, the ThreatQ Platform aggregates and combines unstructured and structured data from any source, internal and external. There's no need to alter existing security infrastructure or workflows; all tools and technologies work seamlessly with the ThreatQ open architecture. No code / low code automation eliminates repetitive, time-consuming tasks so analysts can focus on high-priority and strategic work. The platform also provides flexibility to share curated threat intelligence, advisories and reports with a range of internal and external stakeholders, including manufacturing sectors, quickly.

ACHIEVE MORE WITH THREATQ:

- **CONSOLIDATE** external (e.g., ME-ISAC) and internal (e.g., SIEM) threat intelligence and vulnerability data in a central repository
- **AUTOMATE** enrichment actions in bulk, including correlating data, building relationships, and adding more attributes and context for a deeper understanding of threats and trend analysis
- **ELIMINATE** noise and easily navigate through vast amounts of threat data to focus on critical assets and vulnerabilities
- **SCORE** threat intel sources & manage expiration automatically based on requirements to produce high-fidelity intelligence
- **PRIORITIZE** what matters most for different stakeholders and reprioritize automatically as new data and learnings are available
- **INTEGRATE** with existing tools and threat intelligence sources via a comprehensive library of APIs and custom connectors
- **SHARE** intelligence and respond to requests for intelligence from the SOC and other internal entities right away
- **ACCELERATE ANALYSIS** of attacks and reduce time to create reports and advisories from days to hours

Request a live demo of the ThreatQ Platform and ThreatQ TDR Orchestrator at www.threatq.com/demo.

Sources:

1. IBM Security X-Force Threat Intelligence Index 2023: https://www.ibm.com/reports/threat-intelligence
2. Statista: https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/
3. Dragos: https://cyberscoop.com/ransomware-manufacturing-dragos/
4. Infosec: https://resources.infosecinstitute.com/topics/phishing/phishing-attacks-manufacturing-industry/
5. Blackberry: https://blogs.blackberry.com/en/2023/01/manufacturing-and-cyberattacks-new-research

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.

TQ-IDB10-0324-01

THREATQUOTIENT™

20130 Lakeview Center Plaza, Suite 400 Ashburn, VA 20147 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885