2020 Global Threat Intelligence Report

Understanding your organization's goals, identifying acceptable risk, and building cyber-resilient capabilities are essential to navigating the threat landscape.

Manufacturing cyber-resilience matters

The UK is currently the 9th largest manufacturing nation in the world.[1]

Employs 2.7 million people

Accounts for GBP 275 billion – 45% of total exports

Represents 69% of business research and development (R&D)

'The outbreak of coronavirus has shone a light on the world-leading expertise and capability of UK manufacturing. The inspiring reaction by manufacturers to the government's drive to produce thousands of ventilators and other essential products and materials is testament to the quality of firms and people in our sector. Manufacturers stand ready to help the country through the current crisis in any way they can.'

Tom Crotty, Group Director of INEOS and Chair of CBI Manufacturing Council[2]

Navigate the Manufacturing threat landscape

Our annual **Global Threat Intelligence Report (GTIR)** highlights that Manufacturing is the most attacked business vertical in the UK and Ireland – representing **29% of all attacks.**

Reconnaissance activity was the most common attack type against manufacturers, followed by web application attacks

Reconnaissance activity attacks

Web application attacks

IoT weaponization: IoT devices continue to be compromised

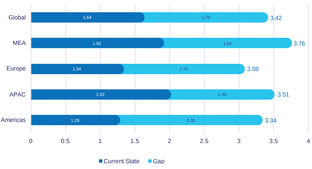
The re-emergence of Mirai and variants has helped widen the spread of IoT attacks – a risk for smart factories and supply chains.

Old vulnerabilities remain an active target

Attackers are still focusing on vulnerabilities which are several years old and have patches available. This trend is particularly problematic in industrial environments, such as manufacturing plants, critical infrastructure production and distribution facilities.

Understand your organization's goals

A gap still exists between the current and desired state for **cyber capabilities in several industries.** Europe's manufacturers lag behind in terms of **process maturity, technology and executive support.**



Closing the gap

In order to close the gap, manufacturing organizations must ensure a **constant focus is placed on:**

01 Maturity of **cybersecurity processes**

02 The correct **tools**

03 **Executive** support

'IDC's research shows that the top inhibitor stopping European security teams from improving their capability is a lack of availability due to time spent maintaining security tools'.

Dominic Trott, IDC's Research Director for Security and Privacy in Europe

OT security requires **a different approach**

Visit the secure OT and IOT page on our website to find out how **manufacturers are using risk assessments** to close their maturity gap and build cyber resiliency. Here are just a few of the services available:

- **visibility of IoT & OT** devices in ICS/SCADA environments (robots, machines, smart tools, sensors)
- secure architecture for production environments
- **security assessments** of ICS/SCADA systems according to ISA/IEC 62443, NIST 800-53v4 and NIST manufacturing **framework**
- **OT Penetration Testing /** Purple Team approach
- security policies for ICS/SCADA environments
- Managed Security Services for ICS

1. The Manufacturer, https://www.themanufacturer.com/uk-manufacturing-statistics/
2. 'Manufacturing output expectations fall amidst COVID-19 outbreak', CBI https://www.cbi.org.uk/media-centre/articles/manufacturing-output-expectations-fall-amidst-covid-19-outbreak-cbi/

Join the conversation

Get the Global Threat Intelligence Report **here**