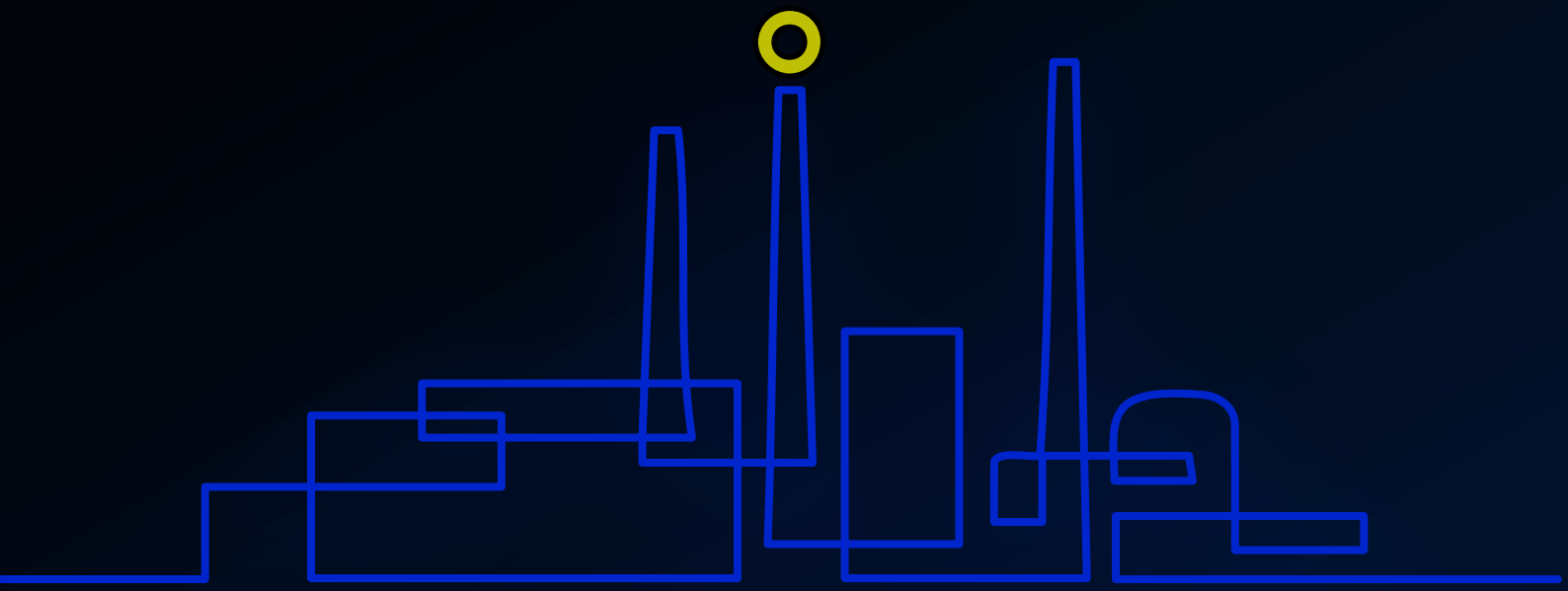
Radiflow

Cyber-Attacks on Manufacturing: A Clear and Present Danger

CIARA, THE FIRST OT-BAS PLATFORM

THE RADIFLOW CYBER-RESEARCH TEAM

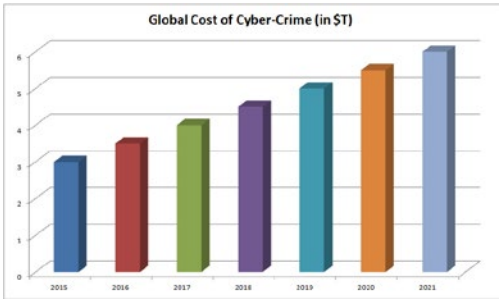


Cyber-attacks on manufacturing: A clear and present danger

A CLEAR AND PRESENT DANGER

Cybercrime is reaching epidemic proportion. The "Official 2019 Annual Cybercrime Report," based on research conducted by Cybersecurity Ventures predicts that cybercrime will cost companies across the world $6 trillion annually by 2021, increasing from $3 trillion in 2015, and would become more profitable than the global trade of all major illegal drugs combined.

The biggest targets are public sector and professional services although in recent years, manufacturing is catching up quickly. According to a Deloitte study titled Manufacturers Alliance for Productivity and Innovation (MAPI), 39% of US manufacturing firms experienced a cyber attack in the past year, of which 38% suffered over $1 million in damages.



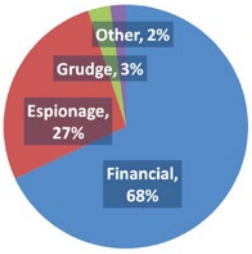
Total global cost of cyber-crime to companies

DAMAGE TO THE BOTTOM LINE

Several major incidents highlight the potential damage that manufacturers face from a targeted cyber-attack.

In early 2019, Norsk Hydro, one of the world's largest producers of light-weight metals, was a victim of a cyber-attack that forced it to halt some production and switch to manual operation resulting in costs of $52 million.

In 2018, TSMC, one of the largest manufacturers in Taiwan, was hit by a cyber-attack that disrupted production resulting in estimated losses of $170 million.

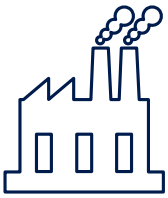


Actor motives in manufacturing attacks (source: Verizon 2019 Data Breach Investigations Report)

The multi-million-dollar impact is the result of downtime in manufacturing capacity which can afterwards extend with a ripple effect in insurance premiums, damage brand reputation, share price and consumer confidence resulting in elevated costs for many years after the event.

RISING THREATS

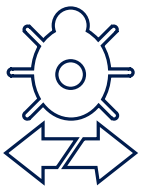
The reason for the growth in attacks against manufacturers stems from several factors:



Industry 4.0 - enhanced automation using software-centric and IoT technologies means more exploit opportunities

Widespread internet-based attacks on manufacturing enterprises (ransomware, crypto-jacking) e.g. the Notpetya ransomware that resulted in $915 million in damages to pharma giant Merck

Proven feasibility of cyber-physical attack models in multiple high-profile examples including Stuxnet (Iran), BlackEnergy (Ukraine) and Triton (Saudi Arabia)



Tools initially developed by nation-state actors to attack critical-infrastructure are now becoming a commodity that is "exported" to the commercial world.

CYBER SECURITY DESIGNED FOR MANUFACTURING

Radiflow's ICS/SCADA-dedicated solutions include an Intelligent Threat Detection System that passively monitors the OT network as well as Secure Gateways that protect OT networks from any deviations from set access policies.

Beyond real-time protection, Radiflow's solution offers a number of network management and optimization features designed around the needs of manufacturing facilities operating multiple business processes:

- Asset Mapping - drill-down visual display of all devices, connections, ports and protocols, as well as each asset's vulnerabilities and risks
- Risk Scoring - based on business process classification and analysis of attack vectors within and between business processes
- Anomaly Detection - using multiple parameters including device sequence sampling time, frequency of operational values and more

For smaller manufacturers with difficulties staffing a dedicated in-house SOC, the Radiflow MSSP model has proven particularly popular and is used worldwide to help protect hundreds of sites.

Radiflow's iSID Industrial Threat Detection System

RADIFLOW'S ICS SECURITY ASSESSMENT

The journey towards better security often starts with an ICS Security Assessment. Conducted by Radiflow's dedicated team of ICS/SCADA cyber-security experts, the assessment starts with non-intrusive network traffic recording, with no interruption to ongoing production (OT) operations. This is used to create a clear, drill-down visualization of the OT network topology including all connected assets along with detection of all known vulnerabilities and analysis of the risks to the customer network with a prioritized risk-mitigation plan.

Radiflow's assessment service is available to manufacturers worldwide - visit our website for more information.

WHY RADIFLOW?

Scalable architecture using Smart Collectors for feeding central iSID analytics servers, as well as iCEN for monitoring multiple instances of iSID

Comprehensive portfolio of detection and prevention tools as well as assessment and monitoring services

Planning value-add: tools for business-driven risk scoring and mitigation planning

Solution maturity: our solutions, designed by industry experts and validated by external labs, protect over 4,000 sites worldwide

ABOUT RADIFLOW

Radiflow develops trusted Industrial Cyber-Security Solutions for Critical Business Operations. Our portfolio of game-changing solutions for ISC/SCADA networks empowers users to maintain visibility and control of their OT networks. Our intelligent Threat Detection and Analysis Platform for industrial cyber-security minimizes potential business interruption and loss within your OT environment.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and automation experts from global cyber-security vendors. Founded in 2009, Radiflow' solutions, are successfully deployed by major industrial enterprises and utilities protecting more than 3,000 critical facilities worldwide. More at www.radiflow.com.

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

France:
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

DACH:
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com