Highlights from the

2019 GLOBAL ICS & IIoT RISK REPORT

A data-driven analysis of vulnerabilities in our industrial and critical infrastructure

Based on analyzing more than 850 real-world industrial control networks via Network Traffic Analysis across multiple industrial sectors and 6 continents

To read the full report, click here

CYBERX

BATTLE-TESTED INDUSTRIAL CYBERSECURITY

www.cyberx-labs.com

The air-gap — still a myth: 40% of industrial sites have at least one direct connection to the internet

Whether for convenience or inattention, many industrial networks continue to be connected to the public internet. With digitization as a key business driver, OT networks, especially in larger companies, are increasingly connected to corporate IT networks as well — further increasing the attack surface and hence the risk.

Broken Windows: 53% of industrial sites have outdated Windows systems like XP

These systems are highly-susceptible to ransomware, destructive malware, and targeted attacks — because they no longer receive patches from Microsoft. But with NotPetya and WannaCry delivering C-level attention to the issue for the first time, we saw a marked improvement compared to 2017.

Hiding in plain sight: 69% have plain-text passwords traversing the network

A lack of encryption in legacy protocols like SNMP and FTP exposes sensitive credentials — making cyber-reconnaissance and subsequent compromise relatively easy.

Anti-anti-virus: 57% of sites are still not running anti-virus protections that update signatures automatically

While owners of critical infrastructure and industrial control systems were once uniformly opposed to anti-virus, many no longer consider anti-virus as disruptive to OT processes, and more and more OT vendors are certifying AV vendors as well.

Indecent exposure: 16% of sites have at least one Wireless Access Point

Poorly configured or misconfigured Wireless Access Points (WAPs) increase the attack surface because they can be accessed by unauthorized clients such as employee or contractor laptops and mobile devices. WAPs can also be compromised via the KRAC WPA2 vulnerability.

Access points such as routers and VPN gateways are also exposed to sophisticated malware such as VPNFilter, enabling attackers to capture MODBUS traffic, perform network mapping, destroy router firmware, and launch attacks on OT endpoints from compromised routers. This means that routers should now be regularly inventoried and patched to prevent these attacks.

Excessive accessibility: 84% of sites have at least one remotely accessible device

Remote management and access protocols like RDP, VNC, and SSH make it easier for administrators to remotely configure devices — but they also make it easier to attackers with stolen credentials to learn exactly how equipment is configured and eventually manipulate it.

Median security scores across all industries: 70%

In 2017, the median overall risk score across all industrial verticals was 61%, with 80% being the minimum recommended score. In 2018 the median overall risk score improved to 70% overall, showing that we're getting better — but still have some ways to go.

67% Manufacturing

68% Pharmaceuticals & Chemicals

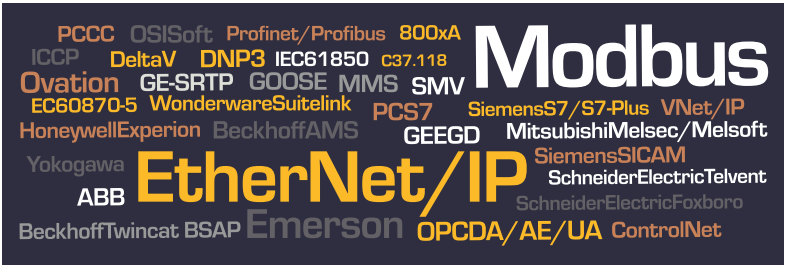
79% Energy & Utilities

81% Oil & Gas

A diverse mix of specialized industrial protocols

Industrial networks contain a complex, heterogeneous mix of specialized OT protocols, which complicates security for OT environments. Traditional IT monitoring tools are "blind" to these protocols, resulting in complete lack of visibility into OT assets, network topologies and activities.

Purpose-built for OT cybersecurity, the CyberX platform incorporates a deep embedded understanding of OT protocols, vulnerabilities, and device behaviors. In our 2018 sample, we encountered a wide range of protocols as illustrated in the word cloud below.



CyberX performed this analysis on an anonymized and aggregated set of metadata with all identifying information removed. The identifiable customer information is separated from data early in the collection process, and rigorous attention is paid to preserving the confidentiality of customer information.

To download the full report, visit https://cyberx-labs.com/resources/risk-report-2019/

ABOUT CYBERX

We know what it takes.

CyberX delivers the only industrial cybersecurity platform built by blue-team experts with a track record defending critical national infrastructure. That difference is the foundation for the most widely-deployed platform for continuously reducing ICS risk and preventing costly production outages, safety failures, environmental incidents, and theft of sensitive intellectual property.

CyberX delivers the only IIoT & ICS security platform addressing all five requirements of the NIST CSF and all four requirements of Gartner's Adaptive Security Architecture. CyberX is also the only ICS & IIoT security company to have been awarded a patent for its ICS-aware threat analytics and machine learning technology.

Notable CyberX customers include 2 of the top 5 US energy providers; a top 5 US chemical company; a top 5 global pharmaceutical company; and national electric and gas utilities across Europe and Asia-Pacific. Strategic partners include industry leaders such as Palo Alto Networks, IBM Security, Splunk, McAfee, Optiv Security, DXC Technology, and Deutsche-Telekom/T-Systems.

Customers choose CyberX because it's the simplest, most mature, and most interoperable solution for auto-discovering their assets, identifying critical vulnerabilities and attack vectors, and continuously monitoring their ICS networks for malware and targeted attacks. What's more, CyberX provides the most seamless integration with existing SOC workflows for unified IT/OT security governance.

For more information, visit CyberX-Labs.com or follow @CyberX_Labs.

CYBERX

BATTLE-TESTED INDUSTRIAL CYBERSECURITY