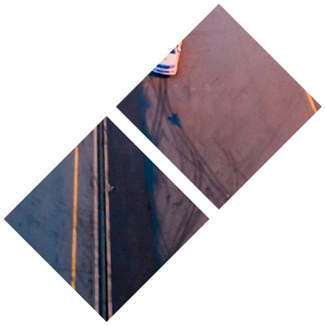
EXECUTIVE BRIEF

The Cost of OT Cybersecurity Incidents and How to Reduce Risk



Cyberattacks can cause devastating business disruptions and lead to financial losses reaching hundreds of millions of dollars.

The World Economic Forum's 2020 Global Risk Report ranked cyberattacks causing disruption to operations and critical infrastructure among the top five increasing global risks.[1] Accenture estimates that the number of cyberattacks has gone up by 67% in the last five years.[2]

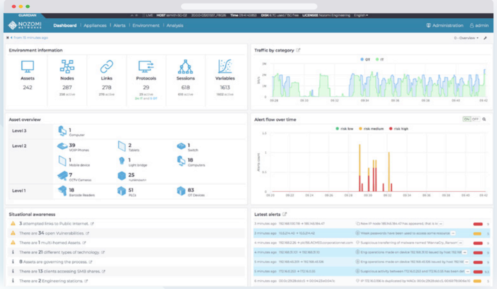
The increasing digital connectivity of industrial networks opens them up to cyber threats, underscoring the importance of protecting not just IT systems, but also operational technology (OT) systems. An analysis of the most prominent cyberattacks that occurred over the past five years across a variety of industries – conducted by Nozomi Networks – shows that OT systems were frequently impacted. Industry sources confirm that regardless of the type of malware deployed, victims suffer business disruption, information loss, revenue loss and equipment damage.[2]

Fortunately, new technology is available that significantly reduces risk by improving the cybersecurity of industrial networks. Simpler to deploy than you might expect, it delivers a nearly immediate ROI.

Improving Enterprise-wide Cybersecurity

While increasing cyber threats dominate the news, there is reason to be optimistic. New technology, such as the Nozomi Networks solution, is easy and safe to deploy, dramatically improves OT/IoT cybersecurity and integrates seamlessly with IT infrastructure.

To see OT and IoT security and visibility in action, and experience how easy it is to work with Nozomi Networks, have your team contact us: **nozominetworks.com/contact**



Environment information

Assets	Nodes	Links	Protocols	Sessions	Variables
242	287 258 active	278 278 active	29 29 active 24 IT and 5 OT	618 618 active	1613 1602 active

Asset overview

Level 3	1 Computer		
Level 2	39 VOIP Phones	2 Tablets	1 Switch
	1 Mobile device	1 Light bridge	18 Computers
	7 CCTV Cameras	25 <unknown>	
Level 1	18 Barcode Readers	51 PLCs	83 OT Devices

Situational awareness

- 3 attempted links to Public Internet.
- There are 34 open Vulnerabilities.
- There are 1 multi-homed Assets.
- There are 21 different types of technology.
- 8 Assets are governing the process.
- There are 13 clients accessing SMB shares.
- There are 2 Engineering stations.

Latest alerts

3 minutes ago	192.168.100.118 → 185.145.184.47	New IP node 185.145.184.47 has appeared, that is kr	9
3 minutes ago	10.5.214.40 → 10.5.214.42	Weak passwords have been used to access some resource	5
4 minutes ago	192.168.2.26 → plc156.ACME0.corporationnet.com	Suspicious transferring of malware named 'WannaCry_Ransom	9
4 minutes ago	192.168.31.101 → 192.168.31.10	Eng operations made on device 192.168.31.10 issued by host 192.168	9
5 minutes ago	192.168.45.201 → 192.168.45.126	Eng operations made on device 192.168.45.126 issued by host 192.168	9
5 minutes ago	172.16.0.253 → 172.16.0.55	Suspicious activity between 172.16.0.253 and 172.16.0.55 has been det	9.3
6 minutes ago	00:0c:29:28:dd:c5 → 00:04:23:e0:04:1c	IP 172.16.0.156 is duplicated by MACs 00:0c:29:28:dd:c5, 00:60:78:00:6a:10	5

High Profile Industrial Cybersecurity Incidents

2016

Duke Energy

Electric Power Company

CYBER COMPLIANCE

Failure to Meet Regulated Cybersecurity Standards

COST

$10 million

Duke Energy Corp. was fined $10 million by the North American Electric Reliability Corporation (NERC) for cybersecurity violations that took place between 2015 and 2018. The 127 violations of safety rules included failure to protect sensitive information on its most critical cyber assets and allowing improper access to sensitive systems and physical locations.

The lapses were considered to pose "a serious risk to the security and reliability" of the power system. Most were self-reported and were attributed to lack of managerial oversight.[3]

2017

A.P. Moller Maersk

Shipping and Logistics

CYBER COMPLIANCE

Ransomware: NotPetya

COST

$300 million

A NotPetya attack disrupted operations for two weeks, blocking access to systems the company relied on to operate shipping terminals. The incident temporarily shut down the Port of Los Angeles' largest cargo terminal. The company lost $300 million in business disruption and equipment damage.

Maersk had to undertake an almost complete infrastructure overhaul. They reinstalled 4,000 servers, 45,000 PCs and 2,500 applications over the course of ten days, a process that would normally have taken six months to implement.[4]

2018

Saudi Petrochemical Plant

Oil and Gas

CYBER COMPLIANCE

OT-Specific Malware: TRITON

COST

Undisclosed

A petrochemical plant in Saudi Arabia, owned by Tasnee, was the victim of a milestone cyberattack that aimed to impact its physical process, by interacting with and controlling its safety system. Fortunately, TRITON's programming led to an automated, safe shutdown of the facility, rather than the intended explosion or uncontrolled disruption.

While the costs of the incident were not disclosed, they included business disruption, process disruption, revenue loss and a major cyber investigation.[5,6,7]

2019

Norsk Hydro

Metals and Mining

CYBER COMPLIANCE

Ransomware: LockerGoga

COST

$70 million

The ransomware LockerGoga blocked the company's systems, forcing a switch to manual operations and workarounds. The Extruded Solutions unit, which makes components for car manufacturing, construction and other industries, reduced its output by 50%.

Administrative systems, such as reporting, billing and invoicing, suffered delays. It took Norsk Hydro several weeks to bring operations back to normal. Lost margins and low production volumes were estimated to cost up to $70 million.[8]

How to Reduce Risk with OT and IoT Visibility and Security Technology

In order to reduce the risk of a cyberattack disrupting business and impacting the bottom line, organizations need to address the cybersecurity risks of industrial systems with the same vigilance they apply to IT systems.

Doing so requires technology that monitors and secures OT networks in real-time. The Nozomi Networks solution is ideal because it is purpose-built and safe for industrial networks, yet integrates easily with existing security infrastructure.

Providing a common platform for both IT and OT teams, the Nozomi Networks solution delivers:

- Superior OT and IoT visibility
- Best-in-class OT and IoT threat detection
- Rapid deployment across many sites

By improving the cyber resiliency of industrial networks and reducing the mean time to respond to cyber threats, the Nozomi Networks solution minimizes the damage and cost of OT cyber incidents.

Meeting and Exceeding Cybersecurity Standards

The Nozomi Networks solution automatically identifies weaknesses in industrial control networks that compromise cybersecurity.

IT/OT teams gain real-time visibility of the industrial network and cybersecurity risks, which helps them improve cyber resilience. Ongoing efforts in this area ensure that an organization is applying the best practices needed to meet and exceed cybersecurity standards.

Detecting and Containing Ransomware

Ransomware is one of the fastest-growing types of cyberattacks, showing a 21% jump in inflicted losses within the past year.[2] The Nozomi Networks solution rapidly identifies known ransomware in industrial systems. Staff are alerted and provided with the OT-specific information and tools they need to quickly contain and mitigate damage.

To make sure risk monitoring is current, the Nozomi Networks solution includes a subscription service called Threat Intelligence™. It delivers regular threat and vulnerability updates created by a team of specialized industrial security researchers.

Identifying and Mitigating OT-Specific Malware

Malware is the costliest type of cyberattack, reaching an average of $2.6 million annually for organizations.[2] The Nozomi Networks solution immediately identifies known OT-specific malware and is regularly updated via the Threat Intelligence service.

In the case of new malware for which no signatures exist, anomaly detection is used to identify suspicious activity.

How to Reduce Risk

Remediation costs and efforts to repair operational and reputational damage can put significant strain on leadership teams. Proactive planning, smart investments in technology, and integration of IT and OT security systems can prevent or reduce the negative consequences of cyberattacks.

More Costs of Prominent Industrial Cybersecurity Incidents

	Organization	Attack Type	Incident and Impact	Cost
Energy	**Ukrenergo** (Ukrainian power company)	OT-Specific Malware: Industroyer/CrashOverride	Disrupted operations resulting in a blackout in the capital city of Kiev.[9,10]	**225K** customers without power
Food & Beverage	**Mondelez**	Ransomware: NotPetya Targeted twice in a year	Lost sales, compromised electronic data plus software and equipment damage.[11]	**$150-$188M**
Manufacturing	**Reckitt Benckiser**	Ransomware: NotPetya	Lost sales, disruptions to manufacturing & ordering systems, shipping terminals, IT networks and other vital infrastructure, in multiple markets.[12]	**$117M**
Pharma	**Merck**	Ransomware: NotPetya	Production shutdown, including inability to fulfill vaccine orders, lost sales and technology remediation.[13]	**$670M**
Shipping and Logistics	**Fedex**	Ransomware: NotPetya	IT operations disruption, impacted deliveries and sales, loss of revenue, and drop in earnings for one quarter.[14]	**$300M**

To see this information online, complete with references, visit nozominetworks.com/cost-of-OT-cyber-incidents

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cybersecurity visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation, building automation and other OT sites around the world. Our innovation and research make it possible to tackle escalating cyber risks through exceptional network visibility, threat detection and operational insight.

nozominetworks.com