NOZOMI NETWORKS

Executive Brief

Business Leaders Need to Quickly Shift Focus to Industrial Cybersecurity

Cyberattacks on critical infrastructure and strategic industrial assets are one of the top five global risks, according to the executives and world leaders who participated in the World Economic Forum's 2018 Global Risk Report[1].

To keep critical systems running and protect the financial results and reputation of your organization, it is essential to improve industrial cybersecurity. Cyberattacks have cost companies millions of dollars through the disruption of services and critical operations. Without visibility and cybersecurity, customer and employee safety are at risk.

Today's business leaders are expected to protect the entire organization beyond enterprise IT systems, including operational technology (OT) environments.

Two of the most important measures you can take to mitigate OT risk are to bring together your IT and OT teams and invest in new technology designed to improve the visibility and cyber resiliency of industrial networks.

Why align IT and OT? Because the technologies they use are converging and their systems are becoming more and more connected. When IT and OT join forces, there is an opportunity to reduce risk and cost, and speed projects.

Why invest in new OT technology? Because it improves reliability, cybersecurity as well as staff productivity and teamwork – and it is much simpler than you might expect, delivering nearly immediate ROI.

Learn how taking these two important steps can help you proactively reduce cyber risks, including damage that could be caused by cyberattacks.

Nozomi Networks Leads Industrial Cybersecurity

- The best solution to manage cyber risk and improve resilience for industrial operations
- > 500 multinational installations in sectors such as critical infrastructure, energy, manufacturing, mining, transportation and utilities

Gartner Cool Vendor

- Nozomi Networks has been recognized for its innovation, impact and intrigue
- Gartner recommends that security and risk management leaders consider new vendors of network security technologies

ARC Advisory Group

- *"Nozomi Networks provides industrial anomaly and breach detection solutions that continuously monitor the health and integrity of critical control systems."*

Enel, Global Energy Provider

- *"With Nozomi Networks SCADAguardian we can now detect and collect operational and cybersecurity issues in real-time and take corrective actions before the threat can strike."*

  Head of Cybersecurity Design, Enel

"80% of the industrial facilities we visit do not have up-to-date lists of assets or network diagrams. The first step to better cybersecurity is better visibility of OT infrastructure. Our solution is easy-to-deploy and combines superior operational visibility and best-in-class threat detection. The ROI is very fast, delivered through increased productivity, enhanced cybersecurity and the use of a common tool for both IT and OT."

EDGARD CAPDEVIELLE
CEO, Nozomi Networks

What is Driving IT and OT Convergence?

The Industrial Internet of Things

The computing landscape of today is characterized by increasing connectivity and data sharing between disparate systems. It also involves data flows between local applications and cloud-based applications, where sophisticated analytics may be done.

Similarly, the Industrial Internet of Things (IIoT) and Industry 4.0 are both trends that involve connecting smart devices and sharing the data they produce to improve existing business models and enable new ones. Benefits include reduced costs, improved productivity, energy savings and faster response to customer demand.

While bringing many benefits, the IIoT also increases cyber risks. Traditionally insecure industrial systems, which include many legacy assets, are now exposed to the type of threats that IT has been dealing with for years. Complicating the picture is the dramatic rise in cyberattacks specifically targeting critical infrastructure and manufacturing systems.

Executive Concerns about Cyber Risks Are Increasing

A 2018 Marsh report[2] found three-quarters of energy executives worry about cyberattacks interrupting their business operations. Physical damage is the cyber loss scenario of greatest concern. As a consequence, most of the executives surveyed are preparing to increase their investments in cyber risk management.

And, both the U.S. and U.K. governments have issued warnings around state-sponsored attacks targeting critical network infrastructure.

Recent examples of the business costs related to cyberattacks on industrial networks include:

- Merck: $780M losses from production shutdown, lost sales and remediation costs[3]
- Maersk: $300M losses from business interruption, lost revenues and remediation costs[4]
- Fed Ex: $300M in lost earning for one quarter, with additional losses to follow[5]

With the IIoT trend increasing cyber exposure for industrial networks, and cyberattacks increasingly becoming the tool of choice for nation states and cyber criminals, losses will likely continue to increase.

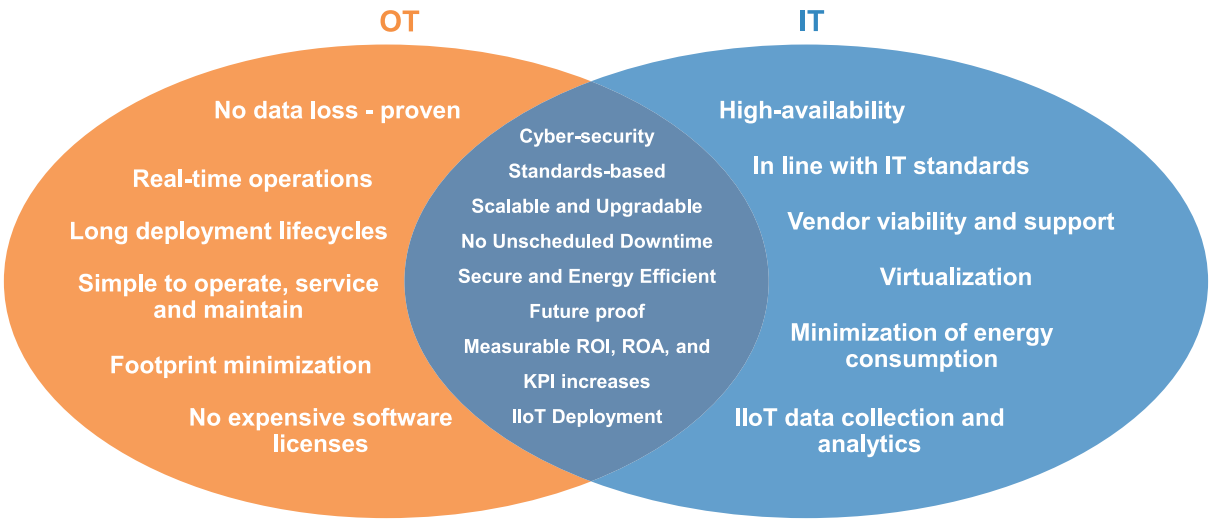
Countering Cyber Risk with IT/OT Convergence

To reduce cyber risks related to industrial systems, it is essential that IT and OT teams combine forces. IT personnel generally have better cybersecurity and cloud expertise, whereas OT staff know how to keep cyber-physical processes running. Collaboration between the groups reduces cybersecurity blind spots and costs.

However, as any initiative that involves people and process, making it happen takes strong direction and ongoing leadership commitment.

Depending upon an organization's convergence maturity level, executives should set appropriate goals. This can include things like having one executive responsible for both IT and OT, facilitating cross-training, and insisting on as much common technology between the groups as possible.

Align OT/IT Priorities to Improve Cybersecurity



Source: Craig Resnick, ARC Advisory Group – reprinted with permission.

Why Invest in the Nozomi Networks Solution?

Solution Designed for OT, Benefits OT and IT

As the cybersecurity risk to critical infrastructure and manufacturing organizations increases, it is important for enterprises to actively monitor and secure OT networks.

An important aspect of this is having complete visibility to OT networks and assets and their cybersecurity and process risks. Until recently, solutions for doing this safely have not been available.

IT solutions do not apply as they do not meet the unique challenges of managing 24/7/365 operational systems where availability is often a bigger concern than confidentiality or integrity.

Nozomi Networks is the OT cybersecurity and visibility vendor of choice because we thoroughly understand industrial networks and processes. Our technology is completely safe for industrial control systems (ICS) and delivers superior visibility, real-time network monitoring and threat detection in a passive, non-intrusive manner. It also integrates seamlessly with IT infrastructure, easily sharing data with existing applications and assets.

Our company has innovated the use of artificial intelligence to automate inventorying, visualizing, monitoring and identifying threats to OT networks. The result is improved cyber resiliency and reliability.

Immediate Value Delivered to Multinational Organizations

Unlike some enterprise-class applications, deployment of the Nozomi Networks solution is straight forward and starts providing ROI quickly. Here is why:

- It's a passive solution that is completely safe for industrial networks and processes.
- It is a mature, 4th generation solution that is ISO9001:2105 certified and quick to deploy.
- It immediately brings benefits by identifying existing threats in the industrial network and improving the productivity of operations and IT staff.

Example Time Savings of One Employee

> *"I slashed ICS administration and cybersecurity labor hours by 10 to 12 hours a week using the Nozomi Networks solution."*
> **Kris Smith, Vermont Electric**

- It readily scales to monitor hundreds of facilities and thousands of devices from a central location.
- It integrates easily with IT/OT infrastructure, supporting existing investments in technology and skills.

Nozomi Networks Benefits for OT and IT: A Safe Solution for OT / Visibility and Detection for IT

OT

A "no process risk" solution that provides comprehensive visibility to all ICS assets

Rapid identification of threats, policy violations and risks to reliability

Unique process views monitor variables such as pump speed or temperature

Faster troubleshooting, as network information is easy-to-see and drill into

Single application that monitors devices from all vendors

A common platform to drive IT/OT convergence

IT

Complete visibility to OT networks and their risk exposure

Consolidated information from multiple industrial facilities via one monitoring tool, when using the CMC

Shows IT-allowed protocols and alerts when disallowed protocols are in use

Faster troubleshooting of OT incidents with ICS-specific dashboards and forensic tools

Seamless integration with SIEMs and other IT applications

A common platform to drive IT/OT convergence

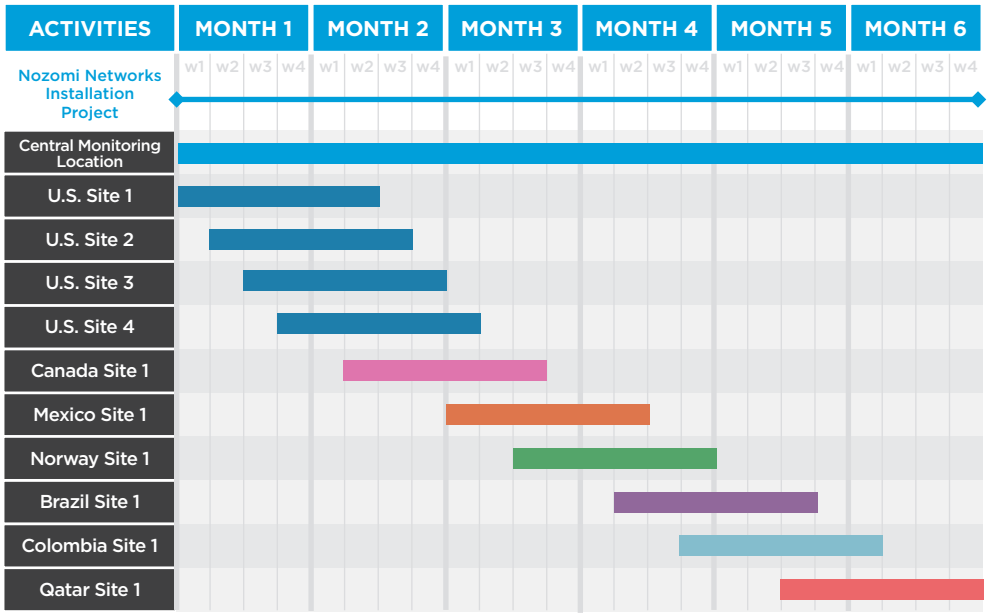
Fast Deployment and Fast ROI for the Nozomi Networks Solution

Sample Deployment

Central Monitoring Location	1
Industrial Facilities	10
Countries	7
Project Duration (months)	6

Implementing the Nozomi Networks solution is time and cost effective, improving:

- OT visibility and cybersecurity
- Reliability
- Productivity
- IT/OT collaboration



Why Choose Nozomi Networks?

Superior OT Asset Discovery and Real-time Network Monitoring

"Nozomi clearly provided the most detail in the asset inventory and was the only competitor to identify the key SCADA system." **S4 Challenge – January 2018**

The Best ICS Threat Detection

"...we chose Nozomi Networks because their platform provides industry-leading capabilities which allow us to detect anomalies and proactively hunt for threats within industrial environments." **Grady Summers, CTO, FireEye**

The Most Global Distributed Installations

500+ hydro-generation plants on five continents | **420+** gas distribution locations | **300+** electric distribution sites

References

1. **"Global Risk Report 2018"**, Weforum.org
2. **"Could Energy Industry Dynamics Be Creating an Impending Cyber Storm?"**, Marsh.com
3. **"NotPetya ransomware outbreak cost Merck more than $300M per quarter"**, Techrepublic.com
4. **"Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk"**, Zdnet.com
5. **"FedEx lost $300 million during Petya attack on TNT Express"**, CIObulletin.com

About Nozomi Networks

Nozomi Networks is the leader of industrial cybersecurity, delivering the best solution for real-time visibility to manage cyber risk and improve resilience for industrial operations. With one solution, customers gain advanced cybersecurity, improved operational reliability and easy IT/OT integration. Innovating the use of artificial intelligence, the company helps the largest industrial facilities around the world See and Secure™ their critical industrial control networks. Today Nozomi Networks supports over a quarter of a million devices in sectors such as critical infrastructure, energy, manufacturing, mining, transportation and utilities, making it possible to tackle escalating cyber risks to operational networks (OT).

NOZOMI NETWORKS

www.nozominetworks.com

@nozominetworks

EB-BUS-LEADERS-A4-002