NOZOMI NETWORKS

The IT Pro's Guide to OT/IoT Security

Digital risk is everyone's business, from the CEO to the end user. Yet in many organizations, it's the IT department that is tasked with managing and minimizing it.

Gartner predicts that by 2023, 75% of organizations will expand their risk management programs to address new cyber-physical systems and converged IT, OT, Internet of Things (IoT) and physical security needs. Today it's less than 15%.[1]

In a world where everything has an IP address and the digital risk surface is expanding exponentially, the IT professional's job has become more difficult and urgent.

Today, the IT team isn't just responsible for securing the large number of personal computing devices used by employees. It is increasingly put in charge of managing and securing mission-critical infrastructure such as Industrial Control Systems (ICS), Operational Technology (OT) systems, cyber-physical systems, and a combination of IT, OT, and IoT devices.

Read this guide to learn how to:

- **Manage unique security challenges** posed by mission-critical operational environments containing IP-enabled devices and complex, interconnected networks
- **Use unified visibility and systems** to stay ahead of risks

More Devices + Automated/ Mission-Critical Systems = Exponentially Higher Risk

This broader scope of operational responsibility creates new challenges for the IT professional. Some of these include:

- Traditional IT security tools and tactics that may disrupt OT, IoT devices and networks, creating the need for new approaches.
- The focus on safety and environmental risks, as well as production and service uptime.
- Increased risks for OT networks because:
  - Many ICS devices cannot be assessed, upgraded or patched due to concerns about disruption and downtime risks.
  - Many OT networks are flat, complicating standard network remediation tactics and allowing malware to spread easily.
  - Meeting compliance requirements is not SOP (standard operating procedure) across ICS networks, as it is for enterprise IT environments.

IT vs. OT Networks: Key Differences

Most IT pros are expert problem solvers. When troubleshooting enterprise IT issues, they typically do so actively – by pinging, scanning, and probing (e.g. running nmap, etc.). And of course, Googling. The challenge for IT pros that now find themselves in charge of OT networks is that most of these tactics no longer work. They may even bring down the network the IT team is trying to troubleshoot.

In fact, a single ICMP packet can easily take down a PLC. And, depending upon what service the PLC is providing, it could become a critical infrastructure disaster. Even the gentlest of pings could translate into a Ping of Death in an ICS network. And because these networks are generally flat and may lack filtering choke points like router ACLs or firewalls, potential issues can quickly scale out of control.

Of course, running a Google search on an ICS issue won't bring down your network. But let's face it – you probably won't find a lot of helpful results for gear that's 10 or more years old.

But wait... what about IoT?

Managing IoT devices is quickly becoming part of the IT team's scope of responsibilities. Whether they're considered mission-critical or not, unmanaged IP-enabled assets like wireless sensors, printers, CCTV cameras, smart TVs, card readers and other devices extend your risk surface area.

If not today, then very soon you'll need to know how to bring these devices under IT control too.

Managing both IT and OT networks means you'll have to work more carefully and creatively than ever before.

Pro-Tip: Get prepared now by learning how to unify security monitoring for everything with an IP address.

The Business Impact of Unique OT and IT Environments

The table below outlines key OT and IT environmental and perception differences, and their impact on organizations. It also provides recommendations on how to effectively manage the disparity.

OT Environment	IT Environment	The Consequences of Unique OT & IT Perspectives	Recommendations for IT Pros
Safety-aware culture; stability and reliability are key concerns (e.g. 'if it works now, don't touch it')	Risk-aware, security-conscious culture; data protection and compliance are key concerns (e.g. 'if it's vulnerable to exploitation, fix it now')	Lack of urgency around cyber risks unless or until they cause downtime; lack of awareness of potential risks for ICS assets	• Learn about differences between OT and IT environments, including taking training on OT-specific networking and cyber security[2] • Spend time with OT colleagues to understand their challenges • Educate your OT team on possible cyber risk threat scenarios and how they might impact uptime and safety • Find out which compliance requirements and security standards apply to your OT[3] and IT networks
High number of unidentified assets, legacy systems, and unmanaged devices	Most assets are known, and are sufficiently managed to reduce risk	The risk surface expands as OT asset management migrates to IT responsibility	• Identify all OT and IT assets, assess for risk and implement defenses and mitigations
Many flat networks, sometimes air-gapped	Highly segmented, multi-homed networks	Lack of connectivity may reduce some risk but contributes to a lack of security visibility and limits threat containment options	• Implement real-time threat detection technology that is safe for OT networks and facilitates fast incident response
Mix of production protocols and insecure communications	Standard TCP/IP protocols; ACLs and encryption protect data in transit	Obscure protocols and insecure communications can be exploited by attackers	• Invest in technology with extensive support for OT and IT protocols, and deep integration with IT/OT environments • Create a baseline of network traffic on OT and IT networks to spot anomalies and address threats that migrate across networks
Downtime and disaster recovery plans that are focused on safety first and business continuity second	Well-established, documented business continuity and disaster recovery plans that prioritize data protection and service resilience	Increased risk of data loss plus untested and unreliable recovery capabilities	• Invest in technology that can deliver unified data protection and support disaster recovery efforts for all assets

The Impact of IT and Industrial Automation Convergence

Integration has become a critical success factor for IT (and IT security) technologies. Thanks to the ubiquitous support of open APIs, many leading applications can feed their dataset into others, enabling seamless and automated workflows. These integrated workflows allow IT pros to work faster and more efficiently than ever before.

Breaking down silos between IT and OT functions reaps enormous benefits, particularly when it comes to deriving insights from data analysis. In fact, while there are multiple factors driving IT and OT convergence, the appetite for data-driven market value is perhaps the biggest driver.

The drive for more data prompts some basic questions, including:

Which assets are on our network?

- What are their specs and operations status?
- How are they configured?
- What are their vulnerabilities, if any?

What are our real-time risks?

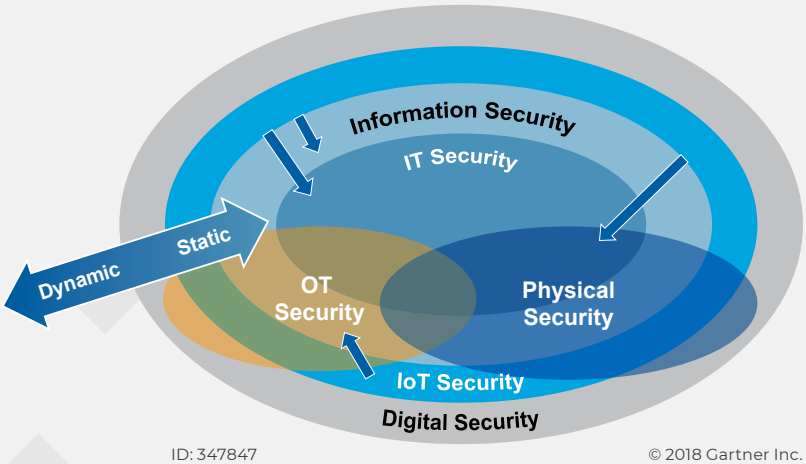
- Downtime risks related to a malware outbreak, human error or other factors – if you can't get to root cause in time, production or safety may be impacted.
- Data breach risks – sophisticated attackers may want to disrupt operations, steal data, or do both. Rapid response is required to stop all threats in their tracks.

What can we do about these risks?

- How do we weave new tools and tactics into our workflow without causing disruption?
- How do we scale security across our distributed environments?
- What procedures do we follow when an outbreak bleeds over from our OT networks to our core IT networks (or vice versa)?

IT/OT Convergence

"To reduce risk, security and risk management leaders should eliminate IT and OT silos by creating a single digital security and risk management function. This function should report into IT but should have responsibility for all IT and OT security."



ID: 347847

"Why IIoT Security Leaders Should Worry About Cyberattacks Like WannaCry," Gartner, January 2018.

To answer these risk-related questions, it helps to consider the People, Process, and Technology factors outlined below.

	Constraints	Consequences	Recommendations
People	Cultural as well as experience and skill-based differences between IT and OT teams. Lack of a common system of record for joint initiatives. Differing priorities.	Without a shared system of record, consensus on metrics, and SOPs, productive coordination and communication between teams remains difficult.	Enable people with training and tools that drive consensus and unify security monitoring across your IT and OT networks by: • Having IT and OT report to a single executive leader. • Cross-training IT and OT teams. • Using a single platform for detecting operational and security risks.
Process	Manual, labor-intensive, and disconnected workflows for cyber incidents that aren't cohesive, and don't feed into each other.	The risk surface expands as OT asset management migrates to IT responsibility.	• Facilitate new processes by using an automated OT and IoT asset inventory tool that provides an accurate network map. Such a tool will help orchestrate workflows for managing risks to all environments.
Technology	Siloed environments and protocol disparity between IT and OT environments (TCP/IP vs. 100s of OT protocols). Traditional tools either lack visibility into or understanding of the OT world.	Most OT networks contain a number of devices that aren't fully identified. Many use outdated and vulnerable software and firmware (which often can't be upgraded). Plus, without appropriate security controls in place, infections from OT networks could bleed into the core IT infrastructure.	• Rely on a technology solution that has been proven to monitor and secure ICS devices at a global scale. Such a solution should detect threats and anomalies in realtime and integrate with IT systems and workflows for fast containment and mitigation.

Top 6 OT/IoT Security Principles

Considering the unique nature of OT networks and the threats facing them, we recommend implementing the following set of core security guidelines:

1. Do No Harm – Public safety is one of the first principles of OT risk management. That's why in many cases, you'll find outdated firmware or software being run in these environments. Many companies view upgrades and patches as having a high risk to safety and availability. Gain consensus on remediation strategies before upgrading everything and asking questions later. Be patient, and remember that some exceptions are worth making, and at the end of the day, everything becomes a risk calculation.

2. Recognize That the Stakes Are High – Mistakes made in managing an OT network may put human lives at risk. They can also bring production or services to a crawl, putting the business at serious financial risk.

An intranet site being down for a few minutes or a few emails stuck in a queue are child's play compared to the potential damage that could be caused by downtime to a critical OT asset. Seek to expand your knowledge of these types of devices and networks, and the risks involved in various use cases. In other words, one size does not fit all.

3. Know What's Normal to Spot What's Not – The assumption underlying most signature-based security tools is that there are a known set of bad things to look for ('known bads'). Everything else is assumed to be innocuous or authorized. Unfortunately, this approach fails to recognize emerging malicious activity and indicators ('unknown bads') that haven't yet been added to signature files, exposing organizations that are at risk. Stuxnet and WannaCry are just two examples of attacks that evaded this threat detection approach and caused billions of dollars in damage worldwide.

Capturing traffic baselines enables faster, broader and more accurate anomaly detection because alerts are triggered for any activity that is outside the norm – regardless of whether the root cause is operational error or cyberattack.

4. Unify Visibility and Destroy Silos – Since cyber attackers typically make lateral moves across a network, it only makes sense to implement a unified approach to security monitoring. Unifying visibility across HQ offices, warehouses, data centers, industrial sites, and field offices destroys blind spots that attackers can exploit, and enables IT pros to maintain a cohesive defense program.

5. Integrate with Existing Products and Processes – Chances are, you've already invested in a variety of IT and security technologies to manage your core IT assets. Rather than disrupt your existing technologies and procedures, look for tools that easily integrate into your organization's systems and workflows.

For example, accommodating technical requirements such as agent installation or cumbersome APIs can extend deadlines and jeopardize project timelines. Additionally, tools that are complicated to manage or aren't easily integrated into your existing workflows are often more trouble than they're worth.

6. Share Insights Across the Business – Gaining unprecedented visibility into your OT and IoT networks will reveal insights that transcend line of business silos. Improved resiliency and security are certainly the start, but in-depth analytics can also shed light on how to optimize operations and increase business value. With this level of visibility, IT pros can offer insights to executives and OT teams that go beyond risk management and lead to positive business outcomes. Ultimately, everyone wins.

Next Steps for Ensuring IT/IoT Security

With IT, OT, and IoT converging quickly across organizations, the next big question is: what short-term and long-term security strategies will help your organization benefit from this trend?

In terms of technology solutions that can help, not all security vendors are up to the task, despite the buzzword-filled claims they might make.

Remember, whether you're concerned about IT, OT, IoT, or IIoT (Industrial Internet of Things), you need to be able to:

- **CAPTURE** asset details and network traffic patterns
- **DETECT** operational failures, threats, and other anomalies
- **ACT** with speed, precision, and insight to maximize business operations

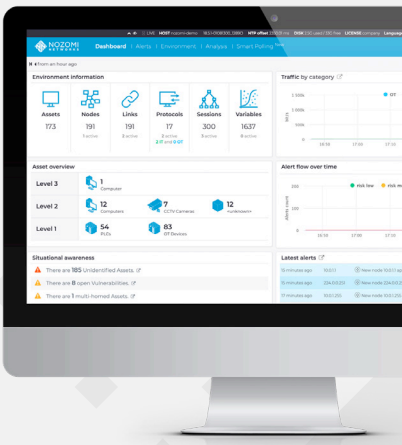
Before you invest in a traditional IT security tool to monitor non-traditional IT gear (ICS, OT, IoT, IIoT, etc.), ask your vendor the following questions:

- How do you manage networks that don't speak TCP/IP and/or can't be connected to trusted networks?
- How do you handle the risk of bringing one of your PLCs offline during production hours?
- How do you discover OT assets that don't respond to ICMP (and may in fact become unresponsive because of a ping packet)?
- What kind of non-TCP/IP protocols can you handle? What process do you follow for expanding protocol support?
- Does your threat intelligence vendor specialize in OT and ICS threats? Which data sources do they use?
- What asset discovery and inventory technology do you use and is it reliant upon an agent or other intrusive tactics?
- What tools do you integrate with? Are your integrations bi-directional in nature?
- Are you able to offer predictive analysis based on baseline activity?

Improving Enterprise-wide Cyber Security

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 cyber security and integrates seamlessly with IT infrastructure.

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



Nozomi Networks: OT and IoT Security for Global Leaders

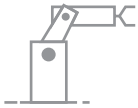
Oil & Gas
6 of Top 20

Pharmaceuticals
5 of Top 10

Electric Utilities
4 of Top 10

Mining
4 of Top 10

Chemicals



Manufacturing

Transportation

Water

Airports

Smart Cities

Building Automation

References

[1] "How to Develop a Security Vision and Strategy for Cyber-Physical Systems," Gartner, 4 April 2019.

[2] SANS Online Cyber Security Training Courses
S4x20 OnRamp Online ICS Security Training Courses

[3] "How the Nozomi Networks Solution Supports the NIST Cybersecurity Framework"
"How the Nozomi Networks Solution Supports the NIS Directive and Regulations"

About Nozomi Networks

Nozomi Networks is the leader in OT and IoT security and visibility. We accelerate digital transformation by unifying cyber security visibility for the largest critical infrastructure, energy, manufacturing, mining, transportation and other industrial 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.

NOZOMI NETWORKS

www.nozominetworks.com
@nozominetworks

LG-IT-PRO-GUIDE-A4-001