CLAROTY

# The Global State of Industrial Cybersecurity

Research Shows that Stronger Operational Technology (OT) Security Yields Stronger OT Availability and Information Technology (IT) Security

# Introduction

Digital transformation is here to stay and is good for business, but it is also creating greater urgency to bridge the cybersecurity gap between Information Technology (IT) and Operational Technology (OT). While IT and OT convergence unlocks business value in terms of operations efficiency, performance, and quality of services, it can also be detrimental because threats — both targeted and non-targeted — now have the freedom to maneuver from IT to OT environments and vice versa.

In this report, we explore the state of OT security from the perspective of IT security practitioners, and provide practical recommendations on how to bridge the IT and OT cybersecurity gap. This report also examines the attitudes and concerns of IT security professionals related to OT security. We asked participants to share their perspectives on a range of topics, including:

- Current safety of industrial networks and critical infrastructure
- Level of concern about cyberattacks on critical infrastructure
- Types of attacks believed to be most prevalent
- Attitudes about training and responsibility for protecting OT networks

While the survey revealed some geographic differences, one area where most IT security professionals surveyed agree is concern over securing OT networks. Despite reporting they have received training and have the required skills, the majority of respondents would rather face a massive data breach than a critical-infrastructure related cyber attack.

This is especially important for Chief Information Security Officers (CISOs) because while digital transformation is shrinking the divide between IT and OT, the historic lack of parity between IT and OT security resources is creating opportunities for adversaries. CISOs have significant catching up to do to lock down their production environments. Part of the challenge has been that traditional IT security solutions are not compatible with industrial control systems (ICS) protocols.  However, this doesn't necessarily mean organizations must make substantial investments in new IT security tools and staffing in order to properly secure their OT environments.

> While digital transformation is shrinking the divide between IT and OT, the historic lack of parity between IT and OT security resources is creating opportunities for adversaries.

## METHODOLOGY

Claroty contracted with Pollfish to conduct a survey of IT security professionals from countries including the United States, the United Kingdom, Germany, France, and Australia. Only individuals who work full time in cybersecurity or information security completed the survey, for a total of 1,000 respondents. The study was conducted during Q4 2019.

# KEY FINDINGS

## I. Assessment of current safety of industrial networks

We began the survey by gathering baseline information to understand regional differences in viewpoints on the state of security of both industrial networks and critical infrastructure.

**Q1. Do you believe that, overall, industrial networks are properly safeguarded?**

**Yes, they're properly safeguarded**

| | |
|---|---|
| 62.30% GLOBAL | 49.00% U.S. |

**No, they need more protection**

| | |
|---|---|
| 37.70% GLOBAL | 51.00% U.S. |

**Q2. Do you believe that your country's critical infrastructure is properly secured against cyber attacks?**

**Yes, we're adequately protected**

| | |
|---|---|
| 59.90% GLOBAL | 45.40% U.S. |

**No, we're vunerable**

| | |
|---|---|
| 40.10% GLOBAL | 54.60% U.S. |

Digging deeper to understand what's driving the numbers up globally, respondents from Australia (93%) and Germany (96%) are much more confident in the overall safety of industrial networks versus respondents from other countries. They are also more bullish that their country's critical infrastructure is properly secured against cyber attacks, with 90% of respondents from Australia and 99% of respondents from Germany saying that they are adequately protected. Meanwhile, U.S. respondents are at the other end of the spectrum, with far less confidence in the security of U.S. critical infrastructure and industrial networks.

The disparity in perspectives points to the need to raise global awareness of attacks on industrial networks. Just as no organization, geographic region or industry is immune to IT security threats, the same is true for attacks on OT networks. For example, NotPetya was devised to spread quickly and indiscriminately outside of Ukraine, and severely disrupted operations of global corporations in the transportation, legal and pharmaceutical industries, among others. Since the Western world had a limited response, we can expect that a more emboldened Russia will reach further.

> Just as no organization, geographic region or industry is immune to IT security threats, the same is true for attacks on OT networks.

## II. Level of concern about cyber attacks on critical infrastructure

A majority of respondents in all regions agree that a cyberattack on critical infrastructure is potentially more damaging than an enterprise data breach. Not surprising then, they are also more concerned about attacks on critical infrastructure.

**Q3. What do you think has the potential to inflict more damage – a cyber attack on critical infrastructure or an enterprise data breach?**

**A cyber attack on critical infrastructure**

| | |
|---|---|
| 75.50% GLOBAL | 67.20% U.S. |

**An enterprise data breach**

| | |
|---|---|
| 24.50% GLOBAL | 32.80% U.S. |

**Q4. What are you more concerned about – a cyber attack on critical infrastructure or an enterprise data breach?**

| | | |
|---|---|---|
| A cyber attack  on critical infrastructure | 73.60% GLOBAL | 65.20% U.S. |
| An enterprise data breach | 26.40% GLOBAL | 34.80% U.S. |

Here again, when compared to their counterparts in other regions, respondents from Australia (91%) and Germany (98%) are much more concerned about cyber attacks on critical infrastructure versus an enterprise data breach. So, while they are very confident in their ability to protect, they also believe that the need to protect is paramount.

High levels of concern about cyber attacks on critical infrastructure among enterprise security professionals around the world align with rising concern among government agencies and law enforcement. The U.S. Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have issued a number of joint advisories warning of Russian nation-state actors with a presence in many critical infrastructure networks. The U.S. Cyber Command has also openly stated that "adversaries direct continuous operations and activities against our allies and us in campaigns short of open warfare to achieve competitive advantage and impair U.S. interests." Their new approach to address an escalation in threats includes "defending forward and continuously engaging our adversaries."

## III. Types of attacks that are of primary concern

When asked about specific threats, respondents put hacking at the top the list of the threats to industrial networks that they are most concerned about, followed by ransomware. There was also a significant consensus that Electric Power and Oil & Gas are the two most vulnerable sectors of critical infrastructure followed by Chemical, Transportation, and Water.

**Q5. What type of cyber attack on industrial networks do you believe will be most prevalent throughout 2020?**

| | | |
|---|---|---|
| Ransomware | 33.20% GLOBAL | 21.40% U.S. |
| Other malware | 13.90% GLOBAL | 10.00% U.S. |
| Hacking/unauthorized network access | 43.20% GLOBAL | 56.20% U.S. |
| Sabotage | 9.40% GLOBAL | 11.80% U.S. |
| Other | 0.30% GLOBAL | 0.60% U.S. |

**Q6. What sector of critical infrastructure do you believe is most vulnerable?**

| | | |
|---|---|---|
| Oil & Gas | 21.60% GLOBAL | 18.00% U.S. |
| Electric Power | 45.10% GLOBAL | 45.60% U.S. |
| Chemical | 12.40% GLOBAL | 11.40% U.S. |

*Q6 Continued from page 4*

| | |
|---|---|
| **Transportation** | |
| 12.30% GLOBAL | 12.60% U.S. |
| **Water** | |
| 6.30% GLOBAL | 9.20% U.S. |
| **Other** | |
| 2.30% GLOBAL | 3.20% U.S. |

With respect to timing and urgency, more than 60% of respondents around the world expect a major attack to occur within the next five years.

**Q7. When will we see a major cyber attack successfully carried out on your country's infrastructure?**

| | |
|---|---|
| **By the end of 2020** | |
| 13.00% GLOBAL | 12.20% U.S. |
| **Within the next 2 years** | |
| 28.60% GLOBAL | 24.00% U.S. |
| **Between 2–5 years** | |
| 25.70% GLOBAL | 26.40% U.S. |
| **Between 5–10 years** | |
| 15.20% GLOBAL | 12.80% U.S. |
| **More than 10 years away** | |
| 5.00% GLOBAL | 6.20% U.S. |

*Q7 Continued*

| | |
|---|---|
| **We don't ever see one** | |
| 6.40% GLOBAL | 10.00% U.S. |
| **It has already happened** | |
| 6.10% GLOBAL | 8.40% U.S. |

Notably, 6.4% of respondents globally and 10% in the U.S. say we won't ever see one.

However, we've already seen ample evidence of attacks targeting energy and other critical infrastructure sectors. The attacks on Ukraine over the last five years are a test case for how a country's infrastructure can be disrupted and paralyzed, and how companies' OT networks can be severely impacted. While OT networks were not the primary target, just the accidental spill-over of NotPetya from IT to OT networks in companies outside of Ukraine should serve as a wake-up call.

## IV. Addressing OT security

Respondents believe that working in IT enterprise security presents more pressure than working in OT security.

**Q8. Which presents more pressure – IT enterprise cybersecurity or industrial cybersecurity?**

| | |
|---|---|
| **IT enterprise cybersecurity** | |
| 66.90% GLOBAL | 58.60% U.S. |
| **Industrial cybersecurity** | |
| 33.10% GLOBAL | 41.40% U.S. |

Yet despite clearly acknowledging the urgency and need for protection against attacks on critical infrastructure, and believing that IT enterprise security is more challenging, the vast majority express little desire to work in industrial cybersecurity.

### Q9. Given the option, which would you rather work in – IT enterprise cybersecurity or industrial cybersecurity?

**IT enterprise cybersecurity**

| | |
|---|---|
| 75.90% GLOBAL | 70.80% U.S. |

**Industrial cybersecurity**

| | |
|---|---|
| 24.10% GLOBAL | 29.20% U.S. |

Perhaps one reason for this is respondents' widely held belief that industrial cybersecurity is not the responsibility of the private sector. In fact, 100% of respondents from Germany believe it is the government's responsibility, followed by Australia (98%), UK (91%) and France (89%) and the U.S. (87%).

### Q10. Is it the government's responsibility to ensure that critical infrastructure is properly protected from a cyber attack?

**Yes, it is**

| | |
|---|---|
| 90.40% GLOBAL | 87.00% U.S. |

**No, it isn't**

| | |
|---|---|
| 9.60% GLOBAL | 13.00% U.S. |

This is where it's imperative that CISOs and IT security teams catch up on the importance of OT security, and how it absolutely does fall into their purview. It is essential to recognize that every company in the world relies on industrial networks. For nearly half of the Fortune 2000 – in industries including oil and gas, energy, utilities, manufacturing, pharmaceuticals, and food and beverage – these industrial networks are critical components to their business. The rest rely on these networks for basic needs like transportation, HVAC systems, lights, elevators, and data center infrastructure. These networks are essential and ubiquitous and, as demonstrated with past attacks, even though not considered part of "critical infrastructure", collateral damage alone can cost companies billions of dollars.

> For nearly half of the Fortune 2000 – in industries including oil and gas, energy, utilities, manufacturing, pharmaceuticals, and food and beverage – these industrial networks are critical components to their business.

Another reason why respondents may rather work in IT security is their comfort level. Answers to the following questions reveal that while they've been trained in the differences between IT and OT networks, believe it is their responsibility to protect these networks, and feel they have the skills, they would rather face a massive data breach.

### Q11. . Have you been trained in the differences between IT networks and OT networks?

**Yes, I have**

| | |
|---|---|
| 75.30% GLOBAL | 65.60% U.S. |

**No, I haven't**

| | |
|---|---|
| 24.70% GLOBAL | 34.40% U.S. |

**Q12. In your opinion, whose job is it to protect an organization's industrial networks?**

| | |
|---|---|
| **IT/Security professional** | |
| 80.20% GLOBAL | 77.60% U.S. |
| **OT manager** | |
| 19.00% GLOBAL | 21.20% U.S. |
| **Other** | |
| 0.80% GLOBAL | 1.20% U.S. |

**Q13. Do you believe you have the skills and experience required to properly manage an OT network's cybersecurity?**

| | |
|---|---|
| **Yes** | |
| 75.00% GLOBAL | 65.40% U.S. |
| **No** | |
| 25.00% GLOBAL | 34.60% U.S. |

**Q14. Should OT-focused cybersecurity be incorporated into the education and training of IT security professionals?**

| | |
|---|---|
| **Yes, it should** | |
| 93.30% GLOBAL | 89.80% U.S. |
| **No, it shouldn't** | |
| 6.70% GLOBAL | 10.20% U.S. |

**Q15. Would you rather work at an organization that experiences a massive data breach, or one that suffers a major critical infrastructure-related cyber attack?**

| | |
|---|---|
| **I'd prefer a massive data breach** | |
| 65.10% GLOBAL | 57.40% U.S. |
| **I'd prefer a major critical infrastructure-related cyber attack** | |
| 34.90% GLOBAL | 42.60% U.S. |

> Respondents largely agree that a cyberattack on critical infrastructure is potentially more damaging than a massive data breach so perhaps, despite their training, they don't feel adequately armed to deal with such an attack.

The 25+ year gap between IT security and OT security may be to blame. Most OT networks have been in place for decades, yet lack even basic security defenses and telemetry that allow security teams to see and monitor these environments, making attacks extremely difficult to detect and mitigate. Furthermore, the teams that run OT environments prioritize availability over security. The risk of disruption and downtime to implement a new security control, a patch or a system upgrade is a non-starter for them. Not to mention that tampering with these multimillion-dollar systems usually voids warranties.

> To feel empowered to secure their OT environments and align with OT priorities, CISOs and IT security teams need asset visibility, continuous threat detection, and secure remote access, that can be easily installed and operated without disrupting productivity or causing downtime.

## RECOMMENDATIONS FOR CLOSING THE IT-OT SECURITY GAP

The benefits of a secure OT environment are far-reaching and compounding. Given the mounting convergence between OT and IT, these benefits include reduced exposure to cyber risks that originate within an OT network but traverse connectivity paths into the IT network. In other words, strong OT security yields stronger OT availability and IT security.

> Strong OT security yields stronger OT availability and IT security.

Another often-overlooked but an impactful benefit, however, is the fact that OT security is a business enabler. CISOs have an opportunity to build on the reputation they've earned supporting digital transformation by creating a strong cybersecurity foundation on the IT side and extending that foundation to the OT side. Here are five actionable recommendations to help CISOs move towards securing OT environments.

**1. Raise awareness for these types of attacks.** The government is taking a more aggressive stance against cyber warfare and the media is shining a spotlight on attacks on industrial networks and critical infrastructure. Every company in the world relies on industrial networks and since cyber has no geographical boundaries, no one is immune to these attacks. Share news and reports to continue to demonstrate that these attacks are escalating in frequency and impact, affecting companies across industries, and are a powerful indicator of what the future may hold.

**2. Educate on the risk of collateral damage.** Although NotPetya did not specifically target OT networks, the attack spread quickly and indiscriminately to companies who likely never thought they needed to concern themselves with these types of attacks. Operations came to a standstill and cost many companies around the globe tens of millions of dollars, if not more, and they were just collateral damage.

**3. Eliminate complexity.** Awareness and education can help you gain support from your board of directors and budget to strengthen the security of your OT networks. The next challenge is to move quickly to close the 25+ year gap between IT security and OT security. OT networks have no modern security controls, so organizations have an opportunity to implement a security program that allows them to focus on what to do next week and next month to reduce risk the most. Instead of starting with a lengthy segmentation project, OT network traffic gives all the security information needed to monitor for threats so start with a solution that you can quickly implement for asset visibility and continuous threat monitoring.

**4. Align IT and OT teams.** The teams that run OT networks prioritize availability. The risk of disruption and downtime to implement a new security control, patch or system upgrade is sometimes a non-starter for them. Not to mention that tampering with these multimillion-dollar systems usually voids warranties. Work together to identify the most important use cases and implement solutions that are agentless and passive, meaning they can be installed without disrupting productivity or causing downtime.

**5. Simplify governance.** Don't fall into the trap of trying to create a separate governance process and security operations center (SOC) for OT security. These efforts usually fail because they are expensive and unrealistic. Ensure the solutions you use integrate seamlessly into existing security solutions -- including Security Information & Event Management (SIEM) tools, Security Orchestration, Automation and Response (SOAR) solutions, analysis platforms, ticketing systems, and firewalls -- and can be operated by IT teams, OT teams, or both.

# CONCLUSION

Protecting industrial networks is a priority for CISOs. Not only must they bridge the decades-long gap in security between OT and IT networks; a gap which is creating heightened risk given the trend in the convergence between OT and IT.

> A strong OT security foundation also enables critical digital transformation initiatives that unlock business value.

However, as this survey revealed, most IT security professionals expressed concern over securing OT networks and don’t feel adequately armed to deal with these types of attacks. IT security professionals need to be empowered with tools that eliminate complexity, align with the needs of OT, and simplify governance. With converged IT and OT solutions, CISOs can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. Strong OT security yields stronger OT availability and IT security and, ultimately, better protection for the networks that run the world’s infrastructure.

Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap. Armed with Claroty’s converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015.

For more information, visit www.claroty.com.

contact@claroty.com

CLAROTY