
# Top 10 Mistakes to avoid in your OT Cybersecurity Uplift Program

By Leon Poggioli
Founder, NetSeg.io
24 February 2026

NetSeg.io

# Top 10 Mistakes to avoid in your OT Cybersecurity Uplift Program

## Introduction

The industrial world is currently undergoing a megatrend, where increased automation and connectivity is radically transforming the cyber risk of industrial environments, which, in turn, creates new risks around safety, operational continuity, and productivity.  OT networks are digitally transforming, and much like the digital transformation of the IT world over the past 15 years, good cybersecurity is fundamental to unlocking this transformation effectively.

Organizations worldwide are investing heavily in OT cybersecurity uplift programs to build resilience, yet many initiatives either fall short of expectations or fail outright. The reasons are rarely a lack of tools or budget; more often, they stem from avoidable mistakes that undermine collaboration, visibility, and sustainable progress.

This guide highlights the **Top 10 Mistakes to Avoid** in your OT cybersecurity uplift program. Drawing from real-world experience across manufacturing, utilities, energy, and other sectors, these pitfalls illustrate the ways that even well-intentioned efforts can go wrong. More importantly, each mistake includes practical ways to avoid them and maximise the probability of success in your program, and in turn, your OT Digital Transformation.

By recognizing these common traps early, you can learn from the mistakes of others, avoid making them yourself, and confidently drive your program forward with great success and less frustration.

## 1. Poor (or No) Collaboration with OT Stakeholders

**Why it's a mistake:**

Without a doubt, cross-functional collaboration is the most critical success factor for OT cybersecurity uplift - which is why it is number 1 on the list.  It has nothing to do with technology - it’s all about the people.  Without effective collaboration and joint program ownership between cybersecurity teams and asset owners, OT teams will become hostile opponents to cybersecurity initiatives rather than valued allies driving the program to success.

Top-down imposition of security without operational owner input on safety implications, operational considerations, or stakeholder engagement means you won’t have the full business context of what needs to be protected and how it needs to be protected.  OT Cybersecurity programs fail without engagement and buy-in from OT stakeholders - treat them accordingly!

**Impact:**

Delayed projects due to lack of co-operation. Technology investments fail to achieve promised ROI due to solutions not being effectively operationalised. Poor alignment means co-ordinating remediation and incident response is difficult or impossible, leading to failed projects after months of frustration.

**How to avoid it:**

Build joint governance and ownership of the initiative - the best projects are jointly owned by Cyber and OT stakeholders from the outset. Let OT stakeholders have a real voice shaping the priorities of the program so they feel in control of the pace and direction while you educate them on the cyber risks that could impact safety and production. Remember where your company makes its money - it's whatever is running on the OT network!

## 2. Assuming an air gap strategy protects your network

**Why it's a mistake:**

True air gaps are almost extinct and only serve to create a false sense of security. Even in isolated environments, connections creep in via USBs, vendor remote access, historians, IIoT, email, or maintenance devices - Stuxnet proved this long ago.

Even if valid, a network isolation strategy does not mean you don't need to monitor that network for unauthorised connections, updates, or the insider threat!

**Impact:**

Having a false sense of security from a stated air gap strategy deprioritizes monitoring, access controls, and segmentation. This makes it easy for attackers to execute their objectives undetected once they can get initial access.

**How to avoid it:**

Recognise the megatrend of every OT network increasing technology and connectivity. Rather than fight it, embrace the digital transformation coming to OT and use this transformation to justify continuous monitoring of OT infrastructure. Map and monitor all connections early and enforce strict controls. Provide corporate-sanctioned access methods for internal and external users, and remove the incentive for non-sanctioned workarounds. For those who stubbornly cling to an air gap strategy, sell them on the idea of continuous monitoring to validate the air gap's integrity.

## 3. Skipping Comprehensive Asset Inventory/Visibility as the first technical investment

**Why it's a mistake:**

You can't protect what you don't see - without a comprehensive understanding of asset inventory, you can't understand what needs to be protected and where the priority risks sit within your OT environment. Showing OT stakeholders an asset inventory also provides enormous operational value and increases their level of engagement in your program.

**Impact:**

Not having a full asset inventory leads to blind spots in risk assessment, segmentation, detection, and response. It's hard to co-ordinate an incident response when you don't have visibility on what is being attacked.

**How to avoid it:**

Recognise and communicate the importance of identifying your OT assets and mapping the network as a starting point of the OT cybersecurity journey. From there, you can build on the asset inventory as a foundation towards greater cyber and operational resilience, doing things like vulnerability management, threat detection, lifecycle management and network segmentation.

## 4. Treating OT Cybersecurity with the same approach as IT Cybersecurity

**Why it's a mistake:**

IT Cybersecurity focuses on the CIA triad of Confidentiality, Integrity and Availability. OT priorities are largely in reverse order: Safety, Reliability and Productivity. Aggressive patching, reboots, IT EDR solutions deployed deep in the network, or auto-updates can cause outages or safety risks, eroding trust and increasing hostility between cyber and operational teams. Incident Response is also very different in OT vs IT, and needs to take business and operational context into account - shutting down a malware-laden server may cause more damage than the actual malware!

**Impact:**

Eroded trust (Caused by walking onto the shopfloor with an IT Cybersecurity approach) makes it difficult to add value and drive a successful program. This approach increases OT team resistance to Cybersecurity initiatives, leading to a lack of co-operation and failed initiatives. In turn, this delays programs and leads to organisations being overly exposed to OT cyber risk due to lack of the co-operation required to drive the program effectively.

**How to avoid it:**

Adapt controls to OT realities, recognise the differences between OT and IT, and maintain strong stakeholder relationships with your OT counterparts. Always seek their point of view of the impact of certain initiatives, and allow them to be your guides on how to best deliver the right cybersecurity capabilities into their environments.

## 5. Inadequate Network Segmentation

**Why it's a mistake:**

Flat networks or weak IT-OT boundaries allow easy lateral movement where an attacker can compromise an IT network and move across to attack the OT network. Assuming that a determined attacker will find a way in, proper Network Segmentation limits the “blast radius” of an attack. Without network segmentation, a single network compromise can give an attacker free run over your entire operational network.

**Impact:**

One IT compromise in a poorly segmented OT environment can lead to full OT access, leading to a major cybersecurity incident that breaks out uncontained. This leads to longer and more costly recovery, and great damage caused from the attack. The SANS state of cybersecurity 2024 highlighted that nearly half of OT cybersecurity incidents occurred as a result of IT compromises pivoting across the IT/OT border to target the OT network.

**How to avoid it:**

Prioritize the IT/OT DMZ layer followed by high-risk zones determined in collaboration with OT stakeholders. Separate devices by function wherever possible, particularly more exposed IoT devices like CCTV cameras, and critical operational devices like Safety Instrumentation Systems (SIS). Implement Purdue Level zoning, 62443 Zones and Conduits, and unidirectional gateways or data diodes where appropriate.

## 6. Narrow Focus on "Pure" OT Assets, Ignoring other devices in OT networks

**Why it's a mistake:**

Securing only pure OT assets like PLCs and SCADA systems while overlooking IT endpoints, IoT sensors, BMS/HVAC, vendor laptops, or third-party gear on the same network means you are open to many more exposed devices that are arguably easier to compromise than pure OT devices.

**Impact:**

Attackers pivot from weak links (e.g., a vulnerable CCTV camera connected on a flat network) to laterally move across to critical OT networks and cause kinetic damage or operational disruption.

**How to avoid it:**

Get holistic visibility and control across the entire IT-OT-IIoT spectrum and recognise the risk each group of assets plays in secure operations - such as CCTV, Building Access Systems, Historians, and Engineering Workstations, for example. Segment different device functions and monitor these systems as a critical control verification.

## 7. Over-Emphasis on Technology while disregarding People and Process

**Why it's a mistake:**

Effective OT cybersecurity programs are all about prioritisation based on risk and ease to implement. Focusing investment on specific tooling won't achieve sufficient risk reduction when basics like policies, training, firewall configurations, and internet-facing devices with default credentials (As seen in the Unitronics attack) remain unaddressed.

**Impact:**

All the technology in the world is wasted investment if not configured correctly. There's no point implementing an OT asset visibility product if it's not regularly used or operationalised to deliver business value. Equally, you'll get more value from discovering basic misconfigurations like default login credentials or firewalls with "any-any" configured as the first rule, than you will from any new technology.

**How to avoid it:**

Focus on the overall program so that investments can be prioritised with foundational hygiene; invest in OT-specific awareness and third-party oversight. Building good cybersecurity awareness and capability at the plant level will increase your ability to drive effective programs, as OT personnel become cyber champions. Good program governance allows for the right investments to be made in tooling, and for those tools to achieve their full business value.

## 8. Weak OT-Specific Incident Response and Recovery planning

**Why it's a mistake:**

Treating OT IR as an IT extension - ignoring operational impacts, physical/safety consequences, or need for manual/local ops during outages makes the incident response less effective and could cause more damage than the actual attack. Equally - looking at OT security operational as a single silo separate from IT security operations could ignore valuable business context.

**Impact:**

Prolonged downtime, amplified business/safety harm; untested plans that fail in a crisis. Risk of the incident response exacerbating the damage caused by the attack, and difficulty co-ordinating incident recovery as different teams begin “finger pointing” over internal mistakes.

**How to avoid it:**

Develop/practice OT-focused playbooks, test backups, ensure manual control capability. Involve OT asset stakeholders in the planning and incident response, and run OT-Specific tabletop exercises to test incident response preparedness. There are 2 schools of thought around separate SOC capability for IT and OT vs a converged model. It is NetSeg’s opinion that a converged model that recognises the difference between these 2 types of incidents is superior to 2 separate SOC functions. Review your Incident Response Retainer (IRR) providers for skills responding to OT incidents and consider reviewing your IRR provider if they lack the required OT Incident Response capabilities.

## 9. Failing to consider remote access as a key threat vector

**Why it’s a mistake:**

Even in allegedly air gapped environments, there is usually some mechanism for external contractors and internal users to remotely access these systems (even if in a “break glass” type scenario). The reality is that most OT environments include a sprawl of different remote access methods using insecure protocols and/or complicated jumpbox environments, with very little governance or oversight on how these methods are being used.

**Impact:**

Lack of control over remote access leading to counterparty risk from 3rd party contractors, and inability to determine root cause when a remote access method is used maliciously.

Equally, blanket banning remote access as a corporate policy leads to insecure shadow workarounds being deployed by site teams and contractors with no malicious intent who want work effectively.

**Avoid it:**

Audit remote access methods currently in use and deploy a flexible, corporate-sanctioned alternative with appropriate auditing and governance so that cyber teams can get oversight of remote access use into OT environments. Standardise on this method and hold 3rd party OEMs to this policy. Consider similar mechanisms for internal users to provide a greater level of governance and avoid shared logins, and to protect systems that may not have any built-in authentication.

## 10. Treating OT Cybersecurity as a point in time project

**Why it's a mistake:**

OT Cybersecurity uplift is a journey. Unlike a firewall refresh, for example, where the Network and Security teams get together, review the market, agree on a path forward, implement and move to operations; an OT cybersecurity uplift project involves years of programmatic work involving risk assessments, visibility and remediation works in a continuous feedback loop, conducted in collaboration with operational stakeholders so as not to impact Safety, Reliability and Productivity. Each stage builds on the learnings of the previous stage, which are essential to drive effective risk reductions.

**Impact:**

OT Cybersecurity projects conducted as "point in time" initiatives more often than not end up with a few discrete initiatives that fall short in delivering what is really needed in terms of long-term capability uplift in terms of people, process and technology. A piecemeal approach with individual small projects will only deliver a fraction of the value that can be unlocked with a co-ordinated program that is considered as an overall journey over a period of several years and budget cycles.

**How to avoid it:**

Recognise that OT cybersecurity uplift requires a long-term programmatic journey, involving multiple stakeholders across different business units (certainly Cyber and OT, and potentially Governance, Safety, Operations, Risk and Compliance). Given the low starting point of maturity for many OT environments, focus on the baby steps first of stakeholder engagement and asset visibility to help determine priorities for subsequent steps.

## Conclusion

Often the best way to ensure success is to invert the problem by identifying obvious mistakes and avoiding them. This guide outlines 10 key mistakes that are often made in OT

Cybersecurity uplift activities, the impact they have on these programs, and how to avoid making them.  By learning from these common mistakes and doing the opposite, practitioners can significantly increase their probability of success in driving an effective OT cybersecurity uplift journey inside their organisation.

The mistakes outlined here, ranging from engaging the wrong people, prioritising the wrong activities, or making investments in the wrong areas, will lead to prolonged exposure, eroded trust, delayed remediation, and, in the worst cases, catastrophic incidents with safety, operational, and financial consequences.

The good news: even a basic grasp of these common mistakes will go a long way to increasing the success of your program. Start with genuine partnership and joint ownership across IT and OT. Build your technical control decisions on a  foundation of comprehensive asset inventory and network mapping. Recognise that while certain controls play a part, they won't achieve the desired outcome without the right people and processes engaged to support the overall program. Above all, commit to the long view with continuous improvement in a feedback loop that respects safety, reliability, and productivity.

By avoiding these top mistakes and adopting a holistic, adaptive mindset, your organization can move beyond internal disagreement, project delays and erroneous assumptions to achieve mature, defensible OT environments that support OT digital transformation rather than add friction to the organisation. The attackers won't wait for you to get your program organised.  Learn from what not to do, and get on the right path to success!

## Call to action

*If you'd like to learn more about how NetSeg.io can help you drive an effective OT cybersecurity uplift program, get in touch with the founder, Leon Poggioli, at leon@netseg.io.*