Research Report

SKYBOX SECURITY

Operational technology cybersecurity risk significantly underestimated

OT faces uphill battle comprised of network complexity, functional silos, supply chain risk, and limited vulnerability remediation options

Contents

- Key findings > 3
- Introduction > 4
- Organizations with OT environments underestimate risk > 6
- Maintaining compliance is a top security concern > 11
- Network complexity increases OT security risk > 12
- Functional silos lead to fragmented security approaches > 17
- Third party risk abounds > 19
- Remediation not a quick fix for OT security > 21
- Exposure risk hides in the labyrinth that connects IT and OT > 23
- Five steps to shore up OT security > 24

Key Findings

Organizations with OT environments underestimate the risk of a cyberattack

Fifty-six percent of all respondents are highly confident that their organization will not experience an OT breach in the next year, yet 83% said they had at least one OT security breach in the prior 36 months. Seventy-one percent of utilities respondents are highly confident they will not experience a breach in the next year, yet 87% said they had at least one OT security breach in the prior thirty-six months.

Apathy is a cybersecurity risk

Forty percent of all respondents said that OT is an afterthought to other digital initiatives.

Maintaining compliance is a top concern

Maintaining compliance with regulations and requirements was the most common top concern of all respondents.

Network complexity increases OT risk

Seventy-eight percent of all respondents said that complexity due to multivendor technologies is a challenge in securing their OT environment. Almost half of CISOs and CIOs said that disjointed architecture across IT and OT pose the greatest security risk in their OT environment.

Functional silos lead to fragmented security approaches

Architects, Engineers, CIOs, CISOs, and Plant Managers agree that functional silos are a top challenge they face in securing OT infrastructure. Over one-third of all respondents said that a top barrier to improving security programs is a lack of central oversight due to decisions made in individual business units.

Third party risk abounds

Forty percent of all respondents said that supply chain/third party access to the network is one of the top three highest security risks. Yet, less than half said their organization as a third-party access policy that applied to OT.

Need to remediate without causing downtime

Seventy-three percent of all respondents said that reliance on manual or ad-hoc scans is challenging. Almost half of CISOs and CIOs said the inability to conduct necessary path analysis across their network to understand exposure is a top security risk to their OT environment. Nearly half of IT Directors/ Managers are concerned about maintaining uptime and availability when implementing remediation solutions.

Introduction

Operational technology (OT) is the backbone of energy systems and other essential utilities, communication systems, building automation, physical security systems, vehicle controls, and more. Despite the criticality of these facilities, the security measures in place on OT products are often weak or nonexistent. The possibility of a breach and the associated financial and reputational damage have not motivated the industry to transform its security programs to date.

Security experts had warned for years that OT systems were sitting ducks and that it was only a matter of time before they came under widespread assault. How did we get here? Most OT assets were not meant to connect to anything in the first place. They were air-gapped, meaning they were physically isolated from non-secure networks. Hence, security was never considered because these machines were isolated islands performing a specific function without wider network connectivity.

However, these machines have now come online with the introduction of advanced sensors, embedded software, Internet of Things [IoT] and Industrial IoT [IIoT] devices, cloud computing, and machine learning. The interconnectivity between IT and OT has improved operational efficiencies in manufacturing to food processing to utilities. Automation, predictive maintenance, and streamlined efficiencies are just a few of the many benefits delivered by the convergence of IT and OT. But this interconnection has also introduced potential risks.

OT is now directly exposed to outside risks via remote sensors to retrieve data, Wi–Fi enabled controllers, and USB devices to update software, for example. Additionally, many producers are starting to sell cloud–based "SCADA–as–a–service" platforms. You could take machines off the IT network to reduce risk, but that would lose the business benefits offered via this connection. Most companies are not willing to do that.

Recently, there has been an alarming rise in attacks on critical infrastructure and other OT systems. Manufacturing is the second most attacked industry, and energy is the third most attacked industry, following the finance and insurance industries.[2] These breaches can inflict physical damage and disable systems that companies and society depend on, threatening bottom lines and life and limb.

Operational technology defined

'Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in asset-centric enterprises, particularly in production and operations.'[1]

[1] *Market Guide for Operational Technology Security,* Gartner, November 5, 2019

[2] *This X-Force Threat Intelligence Index 2021,* IBM, 2021

Top concerns if OT environment experiences a breach

1. Damage to products/services
2. Impact on public safety
3. Loss of contracts, customers, business opportunities

Q: If your OT environment experiences a breach, which of the following three options would you be most concerned about?

The National Security Agency (NSA) and CISA warned: "Over recent months, cyber-actors have demonstrated their continued willingness to conduct malicious cyber-activity against critical infrastructure by exploiting internet-accessible OT assets."[3] OT security has been elevated to a matter of national security by federal authorities. The Biden Administration's Executive Order on Improving Cyber Security, issued in May 2021, explicitly calls out OT—"the vital machinery that ensures our safety"—is an area that must be addressed.[4]

Cybercriminals are all too aware that OT systems are ripe for the picking, and that ransomware attacks on those systems are highly likely to pay off. Companies simply can't afford to have these essential systems disabled, so they're often willing to pay large sums to keep them online.

In fact, organizations with OT environments said product damage, lost business, and impact on public safety were their top concerns if they experience a breach. Yet, these organizations still seem to have blinders on when it comes to their risk of a breach. And the technology, people, and process challenges they will encounter to build a proactive, mature security posture management program are daunting.

Research methodology

Skybox Security fielded a research study in August 2021. The survey was fielded using Qualtrics and respondents were sourced by RepData. The respondents all had decision-making roles within OT security and were blind to who was sponsoring the study.

The research study included responses from 179 OT security decision-makers in the U.S., UK, Germany, and Australia. The majority of the respondents (152) were from companies with $1B or more in revenue within the manufacturing, energy, and utilities industries. The study included a minimum of 30 respondents in the following roles:

+ CISO and CIO
+ Architect and Engineer
+ IT Director/Manager
+ Plant Manager
+ Security Operations Director/Manager

[3] *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems,* CISA, July 23, 2020

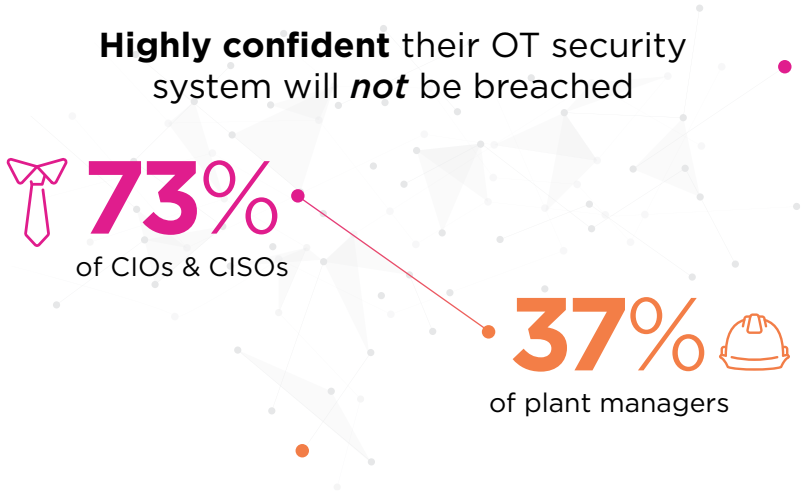
[4] *Executive Order on Improving the Nation's Cybersecurity,* White House, May 12, 2021

Organizations with OT environments underestimate risk of attack

Critical infrastructure is a is not only a lucrative target for bad actors, but it is also a prime target for nation-state sponsored cyberattacks. A major gas pipeline, multiple government agencies, a Florida water supply facility, several hospitals, and the world's largest meat-producing plant are all evidence of the surge in OT attacks. And a 2021 Gartner® report states, "by 2025, attackers will weaponize operational technology environments to harm or kill humans"[5]

New vulnerabilities in OT were up 46% versus H1 2020[6]. These vulnerabilities pose a growing threat to critical infrastructure and other vital systems — a fact made manifest in recent high-profile attacks on facilities, such as oil pipelines, water supplies, and food processing facilities. Threat actors are taking advantage of these OT weaknesses in ways that don't just imperil individual companies – but threaten public health, safety, and the economy.

Despite the rise in vulnerabilities and recent attacks, many security teams do not make OT security a corporate priority. Why? One of the surprising findings is that some security team personnel deny they are vulnerable yet admit to being breached. The belief that their infrastructure is safe — despite evidence to the contrary — has led to inadequate OT security measures. This confusing upside-down world is the Twilight Zone of OT security.



Q: How confident are you that your organization will not experience a breach in the next twelve months?

CISO disconnect between perception and reality

This organizational disconnect starts at the functional level: some roles refuse to believe their OT systems are vulnerable, while others believe the next breach is around the corner. For example, over 73% of CIOs and CISOs are highly confident their OT security system will not be breached in the next year compared to only 37% of plant managers, who have more firsthand experiences with the repercussion of attacks.

[5] Gartner, "Reduce Risk to Human Life by Implementing this OT Security Control Framework", Wam Voster, June 17, 2021.

[6] *Vulnerability and Threat Trends Mid-Year Report,* Skybox Security 2021

> “Some CISOs have false confidence because they’ve already been breached but don’t know it; sometimes hackers are there for a long period of time establishing their foothold. It is **dangerous to be confident** as the bad guys are so good.”
>
> — **Robert Lynch**
> Information Security Manager
> Navistar

One reason why CISOs and CIOs are less aware of OT security risk is that it’s an entirely different domain. While IT focuses on information, OT centers on operations and physical assets. Not only do these organizations have completely different objectives, but they also require very different skill sets.

It is also common for CIOs and CISOs of companies that have not been breached to believe it could never happen; other times, they may have already been hacked but don’t even know it. Increasingly, hackers establish their foothold through less-obvious vulnerabilities and bide their time before causing havoc.

There is also the possibility of an ‘ivory tower’ situation. Unlike CISOs, plant managers are on the factory floor in the trenches working with the machines. They see the potential threat vectors evolving and the sticky notes with password ‘123’ on the plant floor. They know that OT devices are often plugged into the network straight out of the box with default passwords and easily exploitable default settings. They have also seen firsthand the high cost of machine failure and the possibility of devastating injury when something goes horribly wrong due to a breach.

Utility sector's overconfidence foreshadows future breaches

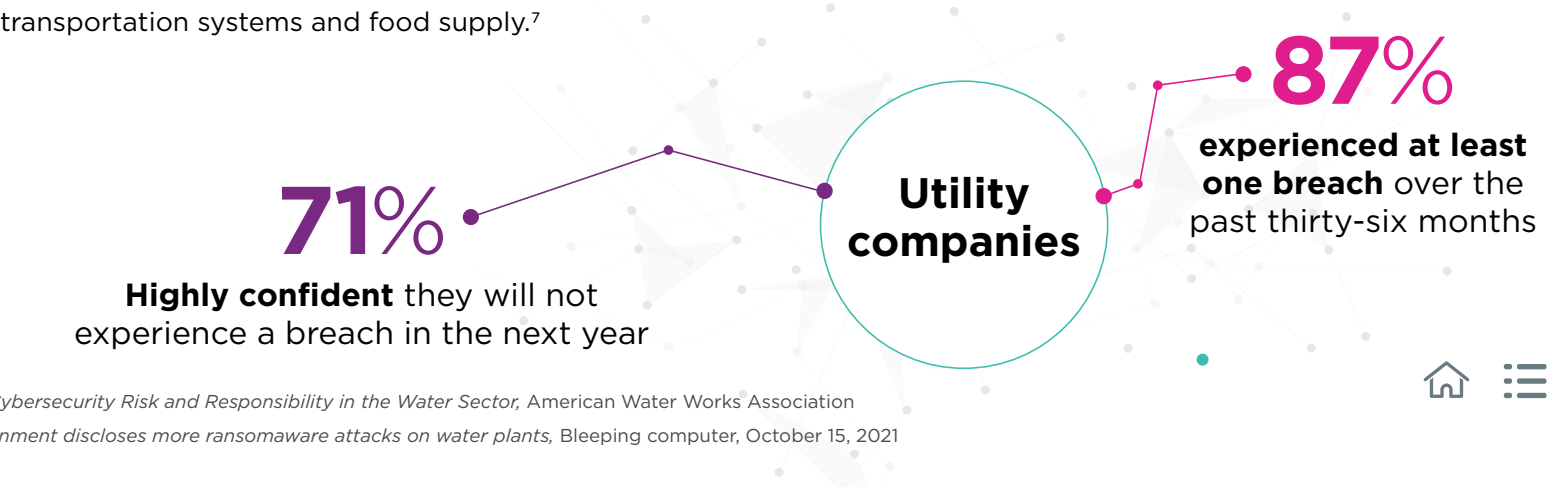
A cyberattack on the nation's utility infrastructure can cause disaster, especially as a part of a fire sale attack that intends to disable or render unusable the nation's transportation, utilities, telecommunications, and financial infrastructure. Surprisingly, 71% of utility organizations are highly confident that they will not experience a breach in the next year. Yet, 87% of utilities companies experiences at least one breach over the past thirty-six months. Utilities are highly regulated and have significant compliance requirements. However, being compliant doesn't necessarily equate to being secure.

The overconfidence of these organizations is curious, considering how high of a target they are. As an example, consider the water sector. Attacks causing contamination, operational malfunction, and service outages could result in illness and casualties, compromise emergency response by firefighters and healthcare workers, and negatively impact transportation systems and food supply.[7]

And these attacks are only increasing. In October 2021, the US federal government advised that U.S. Water and Waste Water Systems Sector facilities have been breached multiple times in ransomware attacks during the past few years.

Multiple ransomware strains were used to encrypt water treatment facilities' systems, including Ghost, ZuCaNo, and Makop ransomware:

+ In August 2021, malicious cyber actors used Ghost variant ransomware against a California-based WWS facility.
+ In July 2021, cyber actors used remote access to introduce ZuCaNo ransomware onto a Maine-based WWS facility's wastewater SCADA computer.
+ In March 2021, cyber actors used an unknown ransomware variant against a Nevada-based WWS facility.
+ In September 2020, personnel at a New Jersey-based WWS facility discovered potential Makop ransomware had compromised files within their system.[8]



[7] *Reduce Cybersecurity Risk and Responsibility in the Water Sector,* American Water Works Association

[8] *US Government discloses more ransomaware attacks on water plants,* Bleeping computer, October 15, 2021

Apathy is a cybersecurity risk

When asked what barriers they face to making security program improvements, 40% of respondents said OT is an afterthought to other digital initiatives. One interpretation is that CISOs responsible for security strategy don't understand the OT environment; therefore, they are not resourcing appropriately. On the other hand, the OT team contributes to cyber security inertia; they care about security risks — just not enough to prioritize them over production goals. Mucking up matters is that IT managers, who are committed to protecting data, do so by constantly patching and updating the entire network; however, this results in production-killing downtime. This political dynamic amongst security team personnel results in a gridlock that stops companies from embracing a more holistic, proactive strategy to protect their OT assets. It's, therefore, no surprise that apathy is perhaps the most significant risk to critical infrastructure security. OT security is now a minimum of 10 years behind IT security, and leaders in the OT space are just now considering centralizing and managing firewalls.

Top barriers
to making improvements to security programs

1. OT is an afterthought to other digital initiatives
2. Decisions are made in individual business units with no central oversight
3. Cyber liability insurance is considered a sufficient solution

Q: Which of the following are barriers to making improvements in your security program?

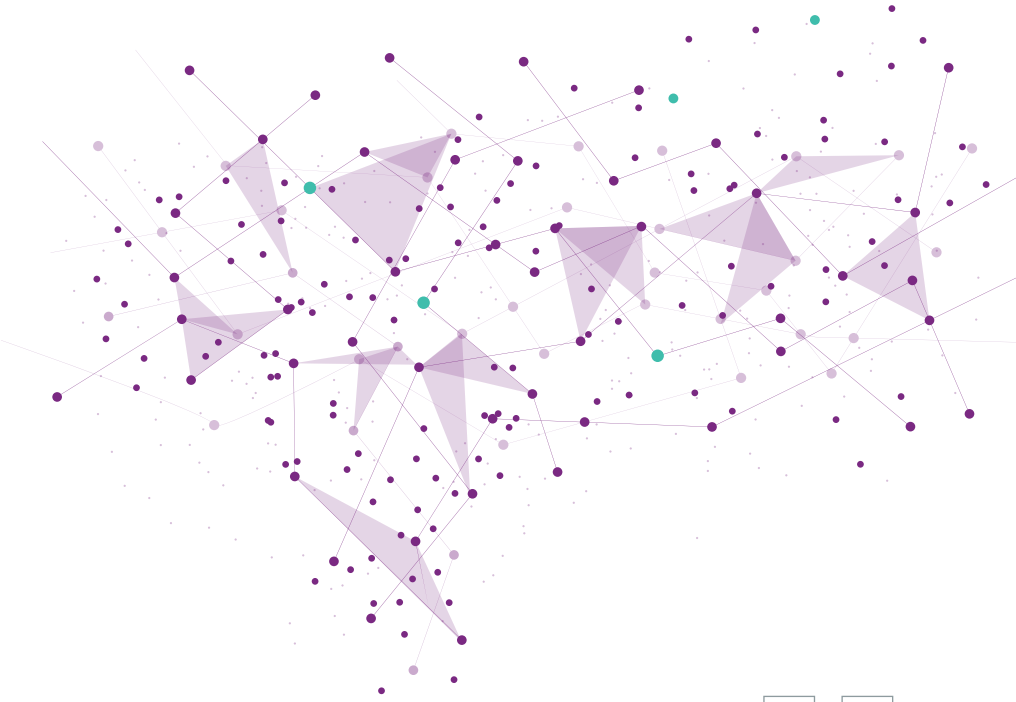
Cyber liability insurance is considered sufficient

Over one-third of respondents said that cyber-liability insurance is considered a sufficient solution. Since cyber liability insurance does not cover costly "lost business," which is one of the top three concerns of the survey respondents, this appears to be a flawed 'security plan.'

The cost of insurance is increasing. Direct written premiums for cyber insurance grew 22% in 2020[9]. Additionally, the costs associated with cyber-attacks continue to increase. The current average is $3.86M per single data breach, with an average loss of revenue totaling $1.52M. The lost business represented the largest share of breach costs at an average total price of $1.59M. Those lost costs included increased customer turnover, lost revenue due to system downtime, and increased cost of acquiring new business due to diminished reputation.[10]

Furthermore, some insurance firms have stopped paying out on cyber insurance claims and others are reducing their coverage. For example, global insurance manufacturer AXA recently announced it will no longer reimburse French companies for ransomware payments.[11]

Indeed, some companies may find cyber liability insurance a "quick fix" — a reactive measure — to solve the more complicated challenge of addressing the real issue with OT security. Unfortunately, cyber liability insurance is not a proactive security strategy, payouts are not guaranteed, and it and cannot protect against long-lasting, costly brand damage. In the long run, building a proactive security posture management program will be less expensive.



[9] *Insurers Must Totally Reassess Approach to 'Grim' Cyber Insurance Market',* Insurance Journal, June 4, 2021

[10] *Cost of a Data Breach Report 2021,* IBM, 2021

[11] *Cyber Insurance FIrms Start Tapping Out As Ransomware Continues to Rise,* Dark Reading, May 24, 2021

Maintaining compliance is a top security concern

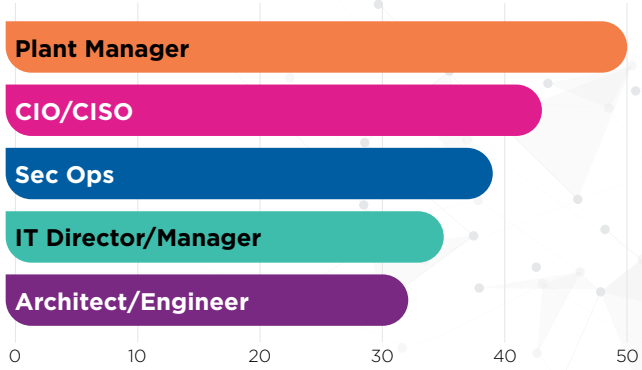
Regulatory compliance requirements are increasing in light of recent attacks on critical infrastructure. For example, this summer the Department of Homeland Security issued security directives that require owners and operators of critical pipelines that transport hazardous liquids and natural gas to implement urgently needed protections against cyber intrusions.[12]

Maintaining compliance with regulations and requirements was the most common concern for all OT decision makers. However, compliance does not equal secure.

It's easy to see why compliance is a concern – it's not easy: mandates often change, are hard to interpret, and are often overwhelming. In the OT environment, security requirements and methodologies are many: STIG compliance requirements, NERC CIP compliance, Compliance with FAIR Methodology, Cyber Value at Risk (CVAR) model. That's a lot of boxes to check.

While maintaining compliance is essential, it is equally important to put measures in place to strengthen your security posture that often extend beyond compliance regulations. Teams who believe that meeting mandates and requirements, like NERC CIP, will make them invincible to an attack can be blindsided by a breach. Compliance, by definition, is meeting the minimum-security requirements for a specific regulation; therefore, a "compliant" infrastructure —without a more resilient security posture — can still be susceptible to a security breach.

One of the key issues that organizations with OT environments face in ensuring compliance is change management. When security and network data are siloed, OT and IT teams can't collaborate and lack the necessary context to ensure accuracy when making changes. The result is blind change management. By taking a proactive security posture management approach, organizations can ensure continuous compliance.



Plant managers are the most concerned about maintaining compliance with regulations and requirements

Q: Please rank the following concerns from greatest to least concern

A: Maintaining compliance with regulations and requirements

[12] *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators,* Homeland Security, May 27, 2021

Network complexity increases OT security risk

Managing OT security is a team sport. If the team members are using different playbooks, they are unlikely to win together. Siloed firewalls, disjointed IT/OT architectures, and disparate security tools have made it impossible to have the insight and context needed to make smart security decisions. Further, the complications of managing a multivendor environment, compounded by the volume of vulnerabilities, make it difficult for IT and OT to prioritize.

Multivendor technologies are a top challenge to OT security

Over 78% of all respondents and 75% of CISOs and CIOS said complexity due to multivendor technologies pose a challenge to gaining full visibility across their attack surface. In addition, 96% of energy and 87% of utilities respondents said the same.

Managing a multivendor environment is challenging. There are simply too many policies and rules to keep track of across devices. Maintaining updates and ensuring proper configurations across a growing deluge of security tools is difficult.

Additionally, each asset often requires a specialist to manage its unique features, so more devices mean more training and consulting costs. In general, each security vendor manages and stores data differently, speaking its own data language working from logs without visibility into the entire network. And with each tool having its unique protocol for when to send an alert, it's nearly impossible to determine which alarms are most critical.

IoT and IIoT increase risk

Over one-third of respondents from companies with over 50,000 employees said the increasing use of IoT or IIoT devices is one of their top three OT security challenges.

This is understandable considering the total number of IoT connections will reach 83 billion by 2024, and the industrial sector will account for 70% of all IoT connections by 2024.[11]

78%

of all respondents said **complexity due to multivendor technologies** pose a challenge to gaining full visibility across their attack surface

[11] *IoT: The Internet of Transformation 2020,* Juniper Research, March 2020

IoT sensors are notoriously vulnerable, giving bad actors plenty of low-hanging fruit to pick. Outdated networks and IIoT sensors ill-designed to withstand cyber attacks have made critical infrastructure a perfect target for cybercriminals. In 2020 alone, IIoT vulnerabilities increased by a staggering 308%[12], reflecting both emergent threats and the rapidly growing use of sensors.

The skyrocketing number of IIoT devices, unscannable assets, and lack of visibility across the attack surface have made it challenging to protect OT infrastructures. IoT devices are so worrisome because they lack critical built-in security controls to defend against attacks. These vulnerabilities allow bad actors to hijack devices to gain wider access to OT networks.

Architecture complexity increases risk

Almost half of CISOs and CIOs said disjointed architecture across OT and IT environments and the convergence of IT technologies are two of their top three greatest security risks. Thirty-eight percent of Architects and Engineers said IT convergence is a top risk, and 42% of Security Operations Directors/ Managers said disjointed architectures are a top risk.

[12] *Cybersecurity comes of age: Vulnerability and Threat Trends Report 2020,* Skybox Security, February 2020

SKYBOX SECURITY

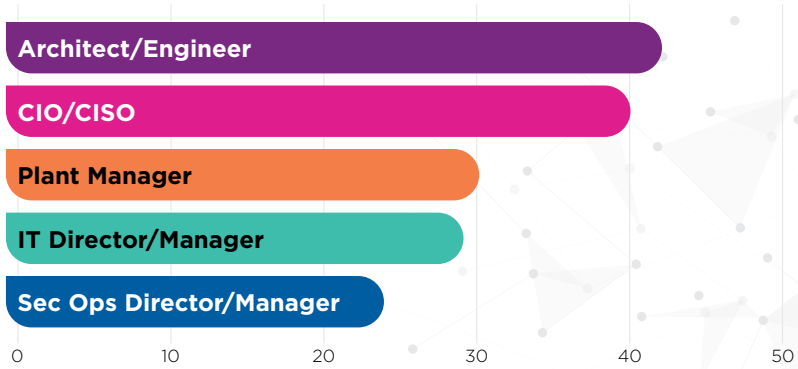
> More organizations are embracing IoT and looking to the future to revolutionize their operations and networks. They must quickly and cost-effectively add thousands of IoT devices or analyze the volumes of data that those devices generate without compromising security. When selecting an IoT device, bear in mind that they are often insecure-by-design. In addition to conducting extensive due diligence on the technology and solutions under consideration, cybersecurity professionals must ensure they effectively assess and manage the cybersecurity risk to the network."
>
> — **Andrea Carcano**
> Co-founder and CPO
> Nozomi Networks

Enterprises have dozens of network security products to keep the IT network secure and running smoothly; however, the data they produce is often disconnected, making it hard to connect the dots. Enterprises also have thousands — even tens of thousands — of vulnerabilities on their network at any given time; policy rules embedded in firewalls, IPS, and other security systems add another dimension.

Because IT and OT each have different teams, technologies, processes, it is difficult to create and maintain security architectures that meet the needs of both groups. This disconnect also creates cracks that attackers can take advantage of to move throughout the organization.

Disconnected architectures make it difficult for teams to assess end-to-end between any two points in a network and between networks — including multi-cloud and OT environments — to identify zone-to-zone access compliance violations, troubleshoot connectivity issues, and spot misconfigurations. Simply put: disconnected architectures mean disconnected data pools. Couple that with manual analysis, and teams can't react fast enough to potential threats and patch necessary vulnerabilities. That's a problem because when exposure vulnerabilities are detected — time is of the essence.

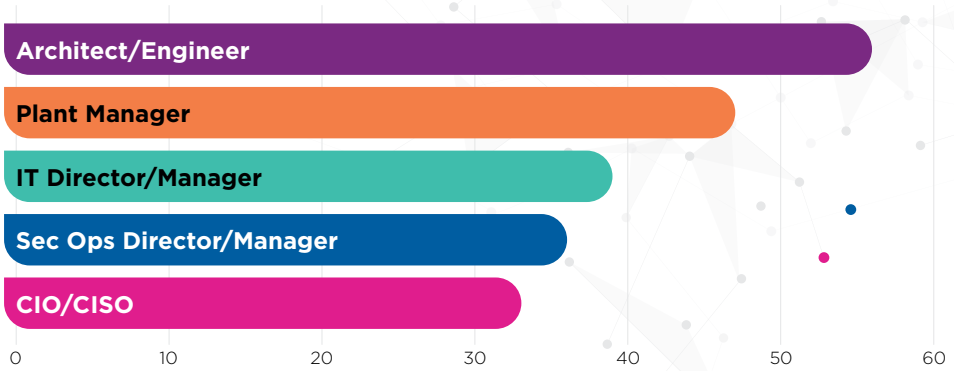
The inability to compare vulnerability data and policy violations across functions makes it near impossible to systematically manage remediation. Without identifying vulnerabilities, misconfigurations, or overly permissive rules, organizations are at an increased risk of a data breach.



Architects and Engineers are most concerned about adhering to security controls in the OT environment

Q: Please rank the following concerns from greatest to least concern

A: Adhering to security controls in my environment



Architects and Engineers say misconfigurations cause greatest security risk to OT environments

Q: Which of the three options pose the greatest security risk to your OT environment?

A: Misconfigurations

Misconfigurations and adherence to security controls cause consternation

In OT, a lack of security awareness and cyber hygiene practices, along with skills gaps, lead to a high propensity for misconfigurations and poorly implemented and managed security controls. It comes down to this: changes to optimize the performance of security controls, such as firewall rules and IPS signatures — to name just a few, need to be made without breaking things. Architects, CIOs and CISOs, in particular, are very concerned about adhering to security controls.

Fifty-six percent of Security Architects and engineers said that one of the greatest risks to their OT environment is that misconfigurations will open their network to bad actors.

Without complete network visibility of the IT-OT attack surface, Architects cannot see misconfigurations, understand vulnerability exposure, identify access policy violations, tackle weak security controls, and improve change management capabilities. Without these insights, companies will be ill-prepared to meet today's Industry 4.0 security challenges.

When poorly configured IT networks meet unpatched OT systems, vulnerabilities spawn, and the chance for breaches increases dramatically. An OT breach can bring production lines to a halt and general business operations to a standstill. For example, the 2017 cyberattack on the pharmaceutical giant Merck disrupted its worldwide operations, including manufacturing, research, and sales operations. This, in turn, led to earnings per share projections dropping significantly. The same malware attacked and crippled global transport and logistics conglomerate Maersk three years later, causing a shutdown of critical systems and $300 million in losses.

The same attack happening twice makes it clear that companies are not taking the proactive security posture management measures needed to mitigate risk. But the lesson is clear: IT security controls and technologies must be properly configured to support security for an OT to avoid infrastructure disasters.

Unfortunately, in complex IT networks, and especially in OT systems, misconfigurations can easily happen. Correct configuration in OT security usually requires specialized knowledge and training; Further, the volume of manual changes can easily lead to human error.

Network segmentation is hard in a complex environment

Network segmentation is an essential security control that can mitigate the risk of attacks across IT/OT converged networks. However, one-third of all respondents said network segmentation is difficult because they have to analyze multiple technology systems. This challenge has proven to be an Achilles heel for organizations with OT environments.

Consider a few of the notorious OT-focused exploits so far:

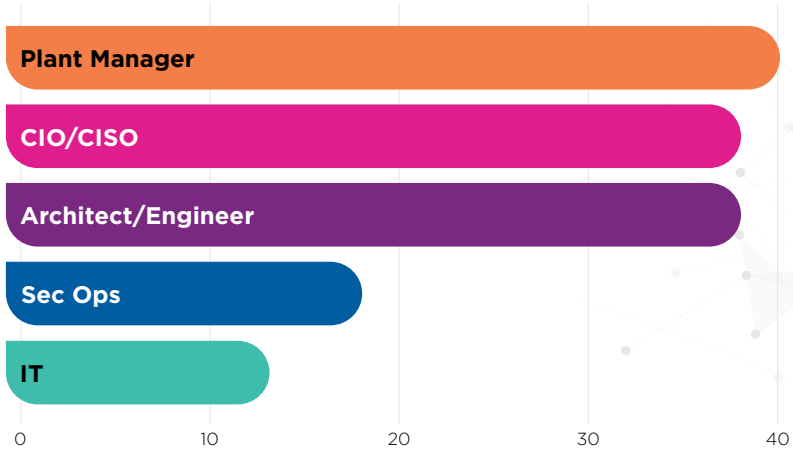
+ In the attack on a water treatment plant in Oldsmar, Florida, hackers attempted to poison the water supply with sodium hydroxide (lye).
+ The Snake ransomware attack shut down Honda's factory operations and global operations, which could have a long-lasting impact on the company's business.
+ The ransomware attack linked to the Russia-based DarkSide cybercrime ring that shut down the Colonial Pipeline in May, resulted in temporary fuel shortages and panic buying in the southeastern U.S.
+ The ransomware attack by another Russia-based organization REvil interrupted operations at the world's largest meat processor (JBS).

In all these cases and many other OT attacks, the hackers gained initial ingress through compromised assets, then moved across networks to penetrate sensitive OT systems. If proper network segmentation had been in place, security teams could block lateral movement and stop attackers in their tracks.

Functional silos lead to fragmented security approaches

When asked to indicate what challenges they face in securing the OT infrastructure, Architects, Engineers, CIOs, CISOs, and Plant Managers selected 'functional silos lead to process gaps and technology complexity' as their top challenge. Unlike their counterparts, IT Directors/Managers and Security Operations Directors/Managers didn't seem to think that functional silos are as big of an issue. Over one-third of all respondents said that a top barrier to improving security programs is making decisions are made in individual business units with no central oversight.

Historically organizations with OT environments were an island. The required functional alignment has not accompanied the technology convergence of IT/OT systems.



Plant Managers and IT Directors/Managers opinions differ greatly when it comes to functional silos

Q: Which of the following are challenges your organization faces in securing OT infrastructure?

A: Functional silos lead to process gaps and technology complexity.

One of the reasons gaps persist is because enterprises working to establish a convergence of IT and OT networks face organizational and process challenges due to separate reporting structures and inconsistent security practices across teams. Most OT network teams typically report to the COO while their IT network counterparts usually report to the CIO. These teams have different goals and approach security from different vantage points.

Additionally, there is a distrust between organizations that have a different set of priorities and approach security from different angles. When IT addresses the security needs of the OT operation, Plant Managers are skeptical, fearing IT will impede their operation — causing downtime — and potentially introduce more risks than solve. This distrust has caused inevitable inefficiencies and widening gaps in OT security. So, what is the solution? When the network world gives you gaps – systematically build a bridge.

> Communication gaps can easily occur. Plant managers don't speak IT, and IT managers often have to learn entirely new skills when working in OT environments. It's important to build bridges.
>
> For example, an IT manager can build a firewall with no rules. Then, the IT manager can show the plant manager what the environment looks like once rules have been applied. The plant manager will increasingly gain trust that the security protocols being put in place will not cause an outage."
>
> — **Robert Lynch**
> Information Security Manager
> Navistar

Third party risk abounds

Forty percent of all respondents said that supply chain/third party access to the network is one of the top three highest security risks. Yet, less than half said their organization has a third-party access policy that applied to OT.

Without having complete visibility into each third-party network, organizations can't know anything about the threats that may be lurking around the corner. As more firms lean on outsourcing to supplement the growing skills gap and help secure their distributed workforce, more security leaders understand the urgency to have visibility into supply chain risk and have the capabilities to mitigate it.

Complicating matters is that many organizations farm out the management of their OT systems to third parties. For example, water utilities often outsource operational work to external contractors, sometimes lacking clarity as to which supplier is working on which piece of the infrastructure.[13] These subsystems in the OT environment are even more vulnerable to malware from third parties.

For example, hackers used a compromised software update from SolarWinds, a network monitoring platform vendor, to access government and other corporate systems. How ironic. If you can't trust a third-party vendor — that has customers ranging from military branches, government to Fortune 500 companies — then who can you trust? This breach proves how unprepared many companies are to monitor their third-party vendors.

40%

of all respondents said 3rd party access is a **top 3 security risk**

Only

46%

said their organization has a **3rd party access policy**

[13] *Water Utilities: Six focus areas to help build cyber resilience,* Ernst & Young, October 4, 2021

Not only are organizations concerned about supply chain risk, but the government is as well. The National Counterintelligence and Security Center (NCSC) issued guidance for supply chain risk management in 2020[14]:

"The increasing reliance on foreign-owned or controlled hardware, software, or services as well as the proliferation of networking technologies, …creates vulnerabilities in our nation's supply chains. By exploiting these vulnerabilities, foreign adversaries could compromise the integrity, trustworthiness, and authenticity of products and services that underpin government and American industry or even subvert and disrupt critical networks and systems, operations, products, and weapons platforms in a time of crisis. We must elevate the role of supply chain security in the acquisition process."

To protect OT systems, security teams need to work together to prioritize the execution of defense-in-depth methodologies. They need to treat every third-party access point along the supply chain with suspicion to prevent malware from wreaking havoc. Tackling this problem starts with an understanding of what security teams can control. Security teams need to be aware of which third-party devices form their attack surface and know what information those devices are sending and receiving.

[14] *Supply Chain Risk Management: Reducing Threats to Key U.S. Supply Chains,* National Counterintelligence and Security Center, 2020

Remediation not a quick fix for OT security

OT environments are often the money makers for the company. Therefore, the idea of introducing downtime to implement security remediation is a big concern as downtime means lost dollars.

> **OT systems** are usually the crown jewels for organizations. They are core systems for **value and revenue creation**. If they go down, they cripple operations.[15]"

'Maintaining uptime and availability when implementing security remediation solutions' is the second most common concern for all respondents, and it is number one for IT and security operation directors/managers. Clearly, IT and security operations directors share the same goal: namely, keep production running.

Remediation is complex because many organizations with OT environments cannot see across their entire attack surface. IT and OT teams need solutions that advance a collaborative approach to prioritize critical vulnerabilities, bolster security resilience, and limit downtime. The key is knowing what network configurations and security controls are in place to include IPS, endpoint security, router ACLs and more. In many cases, patching is not an option, so alternative remediation options need to be available.

When breached, respondents said they took the top three actions: increased security budget; purchased new technologies; streamlined security operations by consolidating tools and teams. Reactive measures can be counterproductive. Purchasing more disparate technology tools can lead to an even more fragmented infrastructure. Increasing a security budget without developing a proactive security posture management program will be fruitless. Consolidating teams without providing them the intelligence and context they need to make better and faster security decisions will not lead to greater security.

Instead, security and IT leaders should develop a common approach to optimize security planning, deployment, and remediation processes to reduce exposure risk. Establishing a proactive security posture management program is the only way to identify and proactively remediate critical attack vectors ahead of the incident.

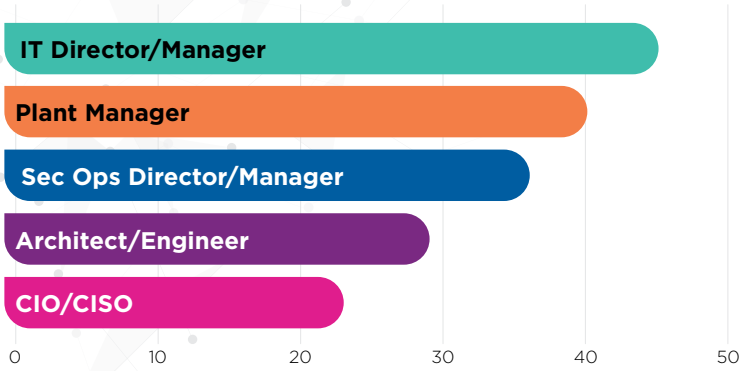
[15] Gartner, "Market Guide for Operational Technology Security", Katell Thielemann, Wam Voster, Barika Pace, Ruggero Contu, January 13 , 2021.

Maintaining uptime and availability is a top OT security challenge

IT and Plant Managers agree that, maintaining uptime and availability is a challenge in securing OT. Interestingly the CIO and CISOs did not feel that this is particularly challenging.

Managing critical infrastructure entails massive environments that can't experience downtime. As a result, OT device vulnerability remediation only occurs around 'once or twice a year, leaving the rear door wide open to nefarious attackers to our critical infrastructure. Since new threats are always evolving, critical infrastructure back doors remain wide open for months rather than being patched when new vulnerabilities emerge.

IT and Plant Managers agree:
maintaining uptime and availability is a challenge



Q: Which of the following are challenges your organization faces in securing OT infrastructure?

A: Maintaining uptime and availability is difficult when making security changes.

When active scanning is not an option, then what?

More internet-connected devices, unscannable assets, and lack of visibility across an extended borderless attack surface have made protecting OT systems challenging. While OT vulnerabilities have become a high-value target for threat actors, those same flaws are often invisible to security teams. That's because many OT systems are hard or impossible to scan. In addition, connected non-IT physical systems (OT/ICS, IoT, IIoT) are often unavailable to scan tools.

A reliance on traditional scan-and-patch methods is often a non-starter when it comes to OT security. When asked what areas pose a challenge to gaining full visibility across the attack surface, 73% of all respondents said reliance on manual or ad-hoc scans. Security teams can't find most OT vulnerabilities using scanning alone, and even if they could, they can't address many of those flaws with patching. In addition, patching can be disruptive to uptime, void warranties, or is impossible for legacy technology no longer supported by the vendor.

Scanning can impact performance or even shut down systems and often requires special passwords and access privileges, which further complicates matters. It's ironic that devices designed to bolster security, such as firewalls and VPNs, are introducing new weaknesses and blind spots into networks. Some enterprise networks have thousands of these appliances in use. Patching all of them would be enormously time-consuming and costly. It would also be a monumental waste of effort since it's typically just a small subset of such devices exposed to attack.

Exposure risk hides in the labyrinth that connects IT and OT

Almost half of CISOs and CIOs say the inability to conduct path analysis across the environment to understand actual exposure is one of their top 3 security concerns. Without shared visibility across IT and OT networks, everyone ends up flying blind in the dark, struggling to fulfill their security responsibilities:

+ IT Directors lack the intelligence and insights to assess, correct and mitigate risks when adding new technology. They struggle with operational complexities because managing separate environments with separate sets of tools results in blind spots.
+ CISOs and CIOs struggle with disjointed architectures, lack of visibility across their OT infrastructure, and worry that misconfigurations will open their network to bad actors.
+ Security Architects can't rely on endpoint security and struggle to reconcile numerous IoT device types, making network segmentation difficult because they can't efficiently visualize and analyze multiple systems.
+ Security Engineers struggle to adhere to security controls because they can't see across their OT infrastructure.
+ Plant Managers don't have visibility and feel helpless to breaches that can impact safety and struggle to maintain uptime and availability when implementing security remediation solutions.
+ Security Operations do not have the insights to know which vulnerabilities to prioritize across multiple vendors and tools.

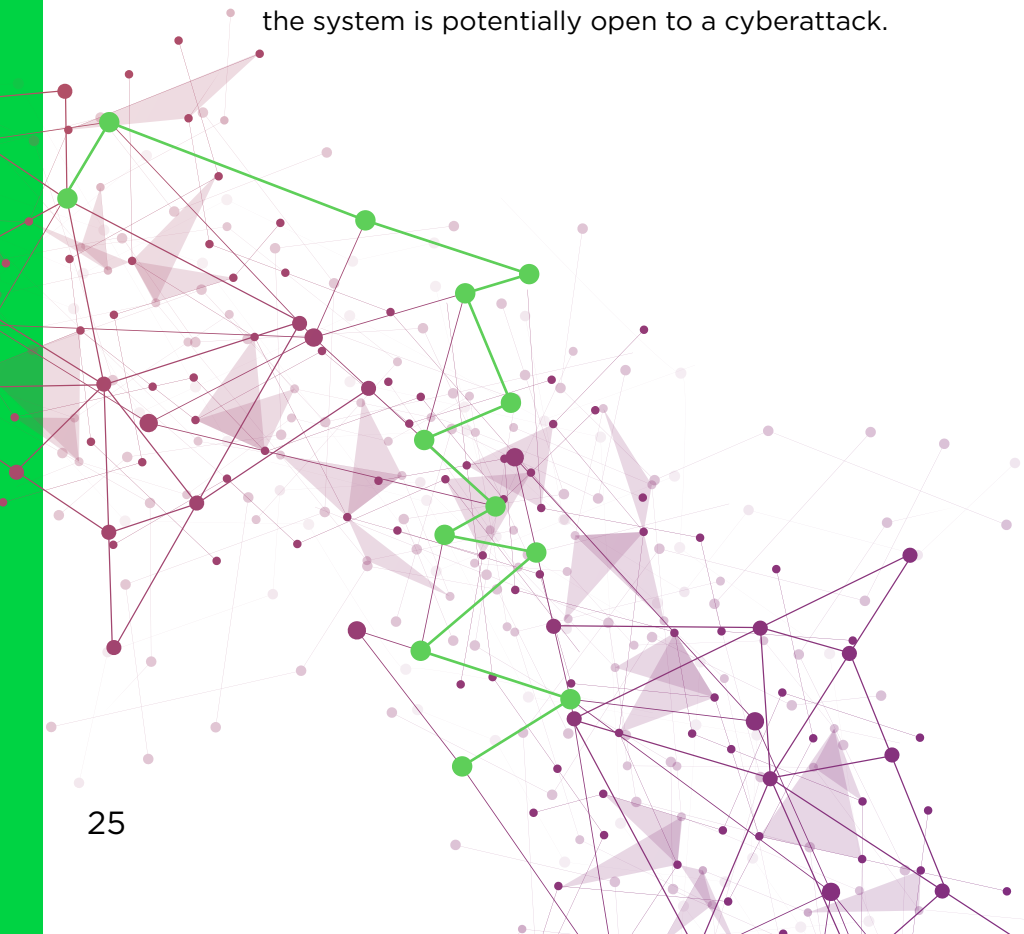
Managing OT security is a shared responsibility. Unfortunately, siloed firewalls and disparate security tools have made it impossible for anyone to have the visibility and insights needed to secure these OT systems.

45%

of CISOs and CIOs say the inability to conduct path analysis...is one of their **top 3 security concerns**

Five steps to shore up OT security

Enterprises need to move from looking in the rear-view mirror toward rigorously managing their security posture to prevent disaster. They need to continuously assess the overall strength of their security controls, processes, and compliance programs and proactively strengthen security efficacy to reduce exposure risks. It is necessary to gain visibility across IT and OT systems, identify and prioritize exploitable vulnerabilities, and correlate this data with unique network configurations and security controls to determine if the system is potentially open to a cyberattack.



Here are five steps companies can take to shore up their OT security:

1 Strengthen security posture management

Because many companies lack a proactive approach to strengthen their security posture management systems, they are often reactive due to an inherent lack of resilience. As a result, IT and security teams are caught in a vicious cycle, spending more money and resources on increasingly ineffective measures and failing to keep pace with the rapidly evolving threat landscape.

What organizations should be focusing on is creating mature, consistent, and enterprise-wide security posture management programs. This joint approach across the IT and OT environments enables leaders to optimize security planning, deployment, and remediation processes to reduce exposure risk. This success is only possible by implementing a network model based on aggregating essential data from a wide range of security, cloud, and network technologies.

2 Implement automation to ensure continuous compliance

The propensity for human error to muck up IT and OT security is a problem that will only worsen. That's because the sheer volume and variation of security controls, rules, and policies needed across a multivendor environment make oversight and change management more difficult. In turn, without the proper updates and configurations, maintaining necessary compliance is impossible. And that's why automation is so critical to maximizing security posture.

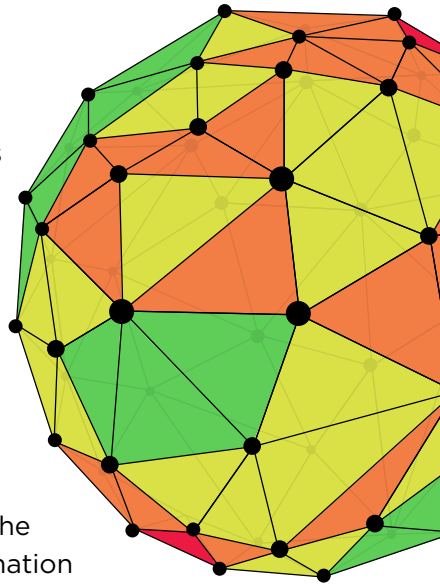
Automating workflows, such as change processes and validation, removes human errors, streamlines operations, and reduces the risk of misconfigurations. Automated closed-loop workflows for firewall rule creation, recertification, and de-provisioning to close security gaps, limit vulnerability exposures, and maintain continuous compliance.

More specifically, automation tools help teams set and adhere to globally applied standards and make sure future changes are compliant. By the same token, automation also allows companies to have multiple compliance requirements and unified in the same platform with a baseline security requirement beyond compliance. For large companies, this type of automation is imperative to identifying network risks.

3 Find exposed vulnerabilities with network model

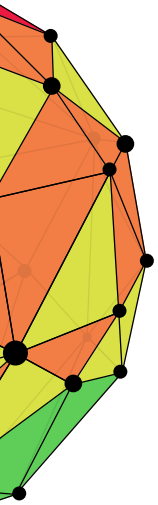
Organizations must see and understand their entire attack surface, including IT, OT, virtual and multi-cloud networks. Illuminating the whole network provides a better, more complete foundation to understand risks anywhere in the organization.

How do you do that?
With a network model.



A network model provides a visualization of all network elements across an organization's various environments combined with an understanding of all the rules and configurations in place. With network modeling, you can run security assessments and simulations against all the devices, vulnerabilities, and configurations within the security environment. Security, IT and OT teams can gain the context needed to implement automation across a wide range of operational security processes. Network modeling provides the insights and visibility needed to perform accurate exposure analysis.

Exposure analysis is a process that identifies exploitable vulnerabilities and correlates them with an organization's unique network configurations and security controls to determine where cyberattacks pose the highest risk. This analysis is only possible with a platform that connects data from configuration, patch, and asset management systems; endpoint security systems; threat intelligence feeds; and various other assets, including cloud, OT, and network security devices. The ability to prioritize the most dangerous vulnerabilities reduces downtime and other operational impacts.



4 Eliminate silos for unified security efforts

Create a standard view, processes, and communications to eliminate silos between security, IT, and plant managers. Security blind spots can be mitigated with the ability to share comprehensive data sets across teams, assets, and infrastructure. This allows for the collection, normalization, and optimization of data sets.

The ability to connect, aggregate, analyze and normalize data across devices enables teams to speak the same security language and work together to find and prioritize critical vulnerabilities to bolster security resilience and limit downtime. By knowing all the paths and firewalls, IT can find what needs to be patched instead of stopping production to unnecessarily patch the entire network.

5 Remediate with options that go beyond patching

When it comes to OT security, there is power in choices. The perfect methodology accomplishes two tasks: identifying the most dangerously exposed vulnerabilities and choosing the best option to remediate these risks. Choices are important because many OT environments have strict policies or concerns when remediating threats and vulnerabilities.

What security teams need today is a solution that calculates risk scores for assets by factoring together four critical variables: the asset's measured CVSS severity; asset exploitability; asset importance; and asset exposure based on the security controls and configurations in place across the network. After accessing how dangerous the risk is to the organization, the next step is to provide prioritized remediation options that include:

+ Applying IPS signatures
+ Modifying access rules
+ Making network segmentation adjustments to block attack paths
+ Updating and optimizing firewall and security device policies/rules
+ Updating and optimizing networking device configurations as needed

Security teams can better protect OT environments when provided a scorecard that highlights the most dangerous risks and the best options to fix them.

The time to reimagine OT security is now

Just as evil thrives on apathy, hackers will continue to exploit OT vulnerabilities as long as inaction persists.

The federal government has taken notice. The Biden administration has called for an initiative to safeguard U.S. critical infrastructure from persistent and sophisticated threats and enhance the energy sector's cybersecurity and its entire supply chain. The U.S. Defense Department and third-party military contractors have prioritized the security of their OT network in the wake of recent security attacks.

Security is hard. However, leaders can overcome complexity with a proactive security posture management program. They will increase accuracy, eliminate downtime, and reduce the risk of compliance fines and hidden costs. Ultimately, they will increase business resiliency and prevent breaches. OT infrastructure is too critical to business, society, and individuals to be left vulnerable.

Interested in speaking with an expert to help solve your greatest security challenges?

Contact us.

skyboxsecurity.com

SKYBOX SECURITY