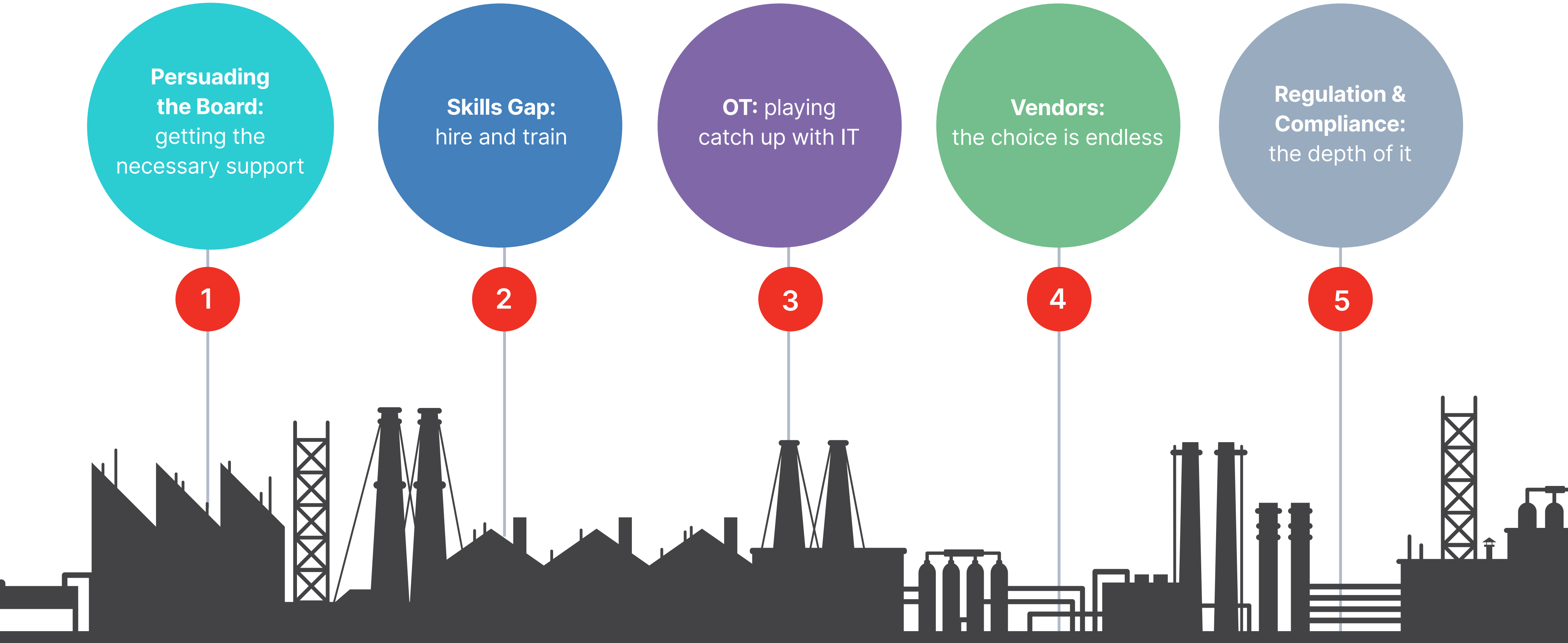
FORTINET

INTERACTIVE EBOOK

5 Issues Keeping OT Experts Up At Night

The Top Challenges in Securing the Energy Sector

High Alert. An apt description of the current state of Operational Technology, especially in the energy industry. There has been an alarming growth in both the size of the attack surface and the range of potential OT targets within critical infrastructure. The potential damage to brand reputation, the financial implications an attack can have, not to mention the human-safety element, are all just some of the factors keeping OT experts up at night.



1. **Persuading the Board:** getting the necessary support
2. **Skills Gap:** hire and train
3. **OT:** playing catch up with IT
4. **Vendors:** the choice is endless
5. **Regulation & Compliance:** the depth of it

Issue #1

> “97% of organizations in the sector had spent less than 1% of their revenue on cybersecurity initiatives.[1]”

Persuading the Board: getting the necessary support

The boards of energy companies must juggle the priorities of today with the needs of tomorrow. The notion of putting big budget towards something that may or may not happen may seem jarring to the board. Regarding cybersecurity, clear and structured risk assessments and metrics are an absolute minimum in the pursuit of budget approval. This can often be frustrating to those on the front lines given the stress of securing the organization. Lack of funds merely worsens the situation.

There is still a conflict between what is in place and what is really needed. As transformation sweeps the sector, certain OT assets will retire. This may lead the board to overlook OT cybersecurity in certain areas, failing to assign the appropriate level of funding required to secure these assets. Yet the need to secure remains, regardless of the operational changes occurring.

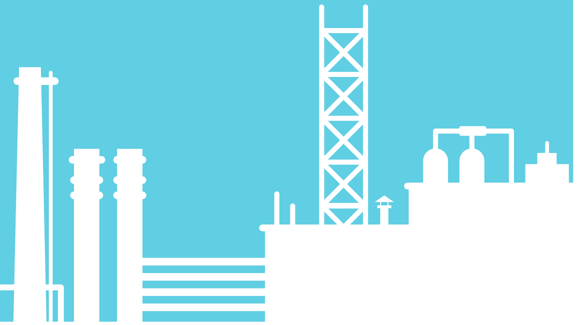
Solution

It is critical to establish board-level oversight. Alignment between different business units and the enterprise-wide risk management framework is also crucial. Companies should adopt a “waterfall approach” for risk mitigation planning and control, which involves defining clear responsibilities for all risk owners and controllers. Having a business continuity plan which has been thoroughly tested, will also be vital in keeping the board satisfied with the cybersecurity finances. In addition, a board appreciates effective metrics that indicate situational status and evolution. Using the Enisa Return on Security Investment framework provides the board clear justifications towards security investments.

How to Convince the Board ☰

Why Fortinet?

With over 20 years of experience in IT and OT cybersecurity, Fortinet deploys Defense-in-Depth with an integrated single-pane-of-glass management and analysis console, decreasing cyber risk, reducing the security burden on OT teams, as well as safeguarding production uptime and safety standards.



Issue #2

“80% of organizations suffered one or more breaches that they could attribute to a lack of cybersecurity skills and/or awareness.[4]”

Skills Gap: hire and train

Hiring in the energy sector is no easy feat. First, it is an industry frequently overlooked by young graduates. Often seen as a conservative and traditional industry, the sector struggles to compete with the Silicon Valley start-up scene or giants like Google or Apple. Secondly, there are few experts who hold the required skillset needed in this industry. The number of cybersecurity experts remains far lower than the demand.

Moreover, the ability to truly understand both IT and OT worlds is reserved to a few highly specialized experts.

If there is an upside to each new attack in the headlines, it’s this: cybersecurity is now firmly on the map as a top industry to work in. Going forward, increased investment and greater internal recognition will hopefully help elevate cybersecurity positions globally.

“The bad guys only have to get through once. The good guys have to protect 24 hours a day, seven days a week”

Joe Robertson, CISO Fortinet.

Solution

Offering generous (and thoughtful) packages

Salary, bonuses, stocks, and holiday packages are one slice of the recruitment pie. Thinking strategically about what would make your organization an attractive employer is perhaps even more key to attracting people.

Hire, then train

Another option is to hire young graduates, offer them training and allow them to flourish in the organization with a clear career path.

Of course, there is a risk that these trained employees will then leave and seek new employment when the demand is high. However, it is a risk which the organization needs to take.

Why Fortinet?

Fortinet Training Institute, an initiative of Fortinet’s Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone.

Increasing cybersecurity awareness should be a firm-wide task and the Fortinet Security Awareness and Training service helps IT, Security, and Compliance leaders build a cyber-aware culture where employees recognize and avoid falling victim to cyberattacks.

Issue #3

OT: playing catch up with IT

The Fourth Industrial Revolution has put technology at the forefront of the energy sector. Converging IT/OT environments helps provide greater productivity, performance, and visibility, as well as reduced production costs and increased revenues. **There are however some fundamental differences between the two environments.**

1. IT cybersecurity and OT cybersecurity teams often have different perspectives, responsibilities, and areas of concern. This can cause friction. Yet, to mitigate attacks and produce efficiency gains, they need to work in harmony.
2. Respective priorities: with IT, security is often a key concern whereas older OT devices tend to be manufactured with little concern for security at all.

Solution

Both IT and OT organizations need to work well together to effectively bring the best security solutions to the OT environment. In the context of differing cultures, both sides are encouraged to get curious and empathetic with one another and to ask ***"Why is it this way?".*** OT organizations that put comprehensive security policies in place give themselves an advantage over threat actors and can limit the impact of a breach. Moreover, testing these policies and having firm governance around this is key to secure OT systems. Organizations must take proactive steps to harden OT environments, including integrating tools and practices designed to protect, detect, and respond to threats in real-time. Micro-segmentation can help with legacy infrastructure, keeping assets as isolated as possible so a compromised system cannot infect other assets.

Why Fortinet?

Fortinet helps secure the convergence of OT and IT as well as having a deep well of IT and OT expertise which can help bridge the cultural gaps within your organization. By designing security into complex infrastructure via the Fortinet Security Fabric, organizations have an efficient, non-disruptive way to ensure that the OT environment is protected and compliant to the NIS Directives.

> "**90%** of intrusions required hours or longer to restore service.[5]"

Issue #4

> “Investment in IT/OT and OT-specific security technologies totaled **$6.9 billion** in 2022.[6]”

Vendors: the choice is endless

The number of attacks is growing and as such the OT security market is growing fast. Organizations often rely on EPCs (Engineering, Procurement, Construction) or OEMs (Original Equipment Manufacturer) to maintain production equipment and make changes. The assets are frequently a ‘black box’ to the owner, who has no insight into the security features or levels of vulnerability. Vendor assessment and contracts for OEMs rarely include a cybersecurity review which makes it difficult to enforce security standards. Even in the cases where security features are included, the buyer will often not use them. This is clearly a severe concern for any energy organization.

Leaving buying decisions to an EPC or OEM can deprioritize the security element. Even if a vendor or third party has sufficiently been vetted, that does not ensure security across the value chain. One needs to have a zero-trust mentality: assume any connection is a threat until proven otherwise. A proactive stance via procurement policies towards security is imperative, with strict requirements for every member of the value chain being essential.

Solution

To have security across vendors, you need to have a security provider who can go across vendors. Do not accept security ‘as is’. If the responsibility of security lies outside of your organization, your organization does not have complete control of it.

For converged networks, an ideal IT/OT security solution’s top requirement are to:

- Identify assets, classify them, and prioritize value
- Segment the network dynamically
- Analyze traffic for threats and vulnerabilities
- Secure both wired and wireless access
- Have mechanisms to deal with threats both known and unknown

Why Fortinet?

The Fortinet Security Fabric provides an organization with a comprehensive portfolio of security tools that can protect its operational technology resources.

With it, you get a proactive approach to securing your OT. There is no need to source multiple security devices to patch weaknesses or protect desperate assets. The Fortinet Security Fabric ensures all assets within your IT and OT ecosystems get the protection they need.

Issue #5

Regulation & Compliance: the depth of it

Staying compliant in the energy sector is no simple task. It takes time and an extensive knowledge of the entire organization. To become certified often requires a great deal of due diligence. To address the increase in OT and IT threats, Gartner expects global governments and organizations will take even more actions on security.[8]

To stay compliant, full awareness of what is to come is key. Consolidation in these standards across the energy industry will become the new normal, helping to simplify the numerous regulations that exist at a national and international level.

> "Nearly 1/3 of nation-states will pass legislation to regulate ransomware payments, fines, and negotiations through to 2025; in 2021 that number was less than 1%.[7]"

Solution

Understanding the depth and staying up to date with regulations is an obvious minimum for any energy organization. The NIST Cybersecurity and MITRE ATT&CK® ICS frameworks serve as a critical basis for mitigating the risks of IT/OT convergence in the energy sector.

Regulations/Frameworks list

Why Fortinet?

Fortinet aligns to these standards and guidelines. The deployment of a comprehensive, updated cybersecurity system with a mature governance framework must include a high level of IT/OT collaboration, as well as executive management support behind it all. The MITRE ATT&CK for ICS Framework is incorporated into Fortinet's analysis and management products as well as help providing a dedicated team to help support at every step of the way.

Conclusion

These five issues are all significant and underpin the various problems faced by OT organizations in the energy sector. The current climate has set alarm bells ringing across the industry. These will hopefully put security at the forefront of not just production organizations but the market as a whole. Fortinet is the only vendor that can deliver a truly integrated Security Fabric that covers both IT and OT security best practices and requirements for the entire converged IT/OT environment. Fortinet has a strong track record protecting critical infrastructure and is a strategic partner for any OT organization.

Find out more about how Fortinet can help solve your issues today.

DISCOVER MORE

On the energy industry:

US$4.4m

Amount paid by Colonial Pipeline for a ransomware attack in 2021. [9]

Energy is most-at risk industrial sector for cyberattacks

According to a 2021 SANS report.[10]

1. EY: How digital transformation must go in hand with cyber resilience
2. 2022 The State of Operational Technology and Cybersecurity
3. Idem
4. 2022 Cybersecurity Skills Gap – Global Research Report
5. 2022 The State of Operational Technology and Cybersecurity
6. Idem
7. Gartner Reveals Top 8 Security Predictions for the Next 5 Years
8. Idem
9. Accenture 2021 Cyber Threat Intelligence Report
10. A SANS 2021 Survey: OT/ICS Cybersecurity

www.fortinet.com

November 9, 2022 1:50 PM
1837153-0-1-EN

Issue #1

“97
orga
in th
had
than
their
cybe
initia

Persuading the Board: getting the necessary support

The boards of energy companies must juggle the priorities of today with the needs of tomorrow. The notion of putting big budget towards something that may or may not happen may seem jarring to the board. Regarding cybersecurity, clear and structured risk assessments and metrics are an absolute minimum in the pursuit of budget approval. This can often be frustrating to those on the

ack of funds merely worsens the situation.

hat is really needed. As transformation
ay lead the board to overlook OT
ropriate level of funding required to secure
ss of the operational changes occurring.

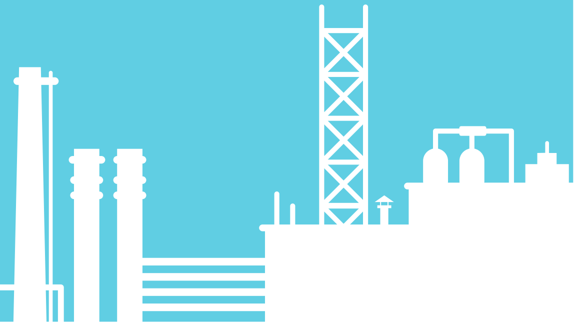
- **Business and financial impacts:** An attack can have a huge impact on business. A recent survey stated that nearly 93% of organizations had at least 1 intrusion in the past year and 78% had at least 3.[2]
- **Security Gaps with Point Products:** OT security is gradually improving, but security gaps still exist in many organizations. The SANS report found that a vast majority of organizations use between two and eight different security vendors for securing their industrial devices. Many have between 100 and 10,000 devices in operation. This complexity will challenge any IT security team using multiple OT security tools that are not integrated. It also creates gaps in their cyber defences and invites attacks.
- **Lack of Centralized Visibility:** Without the centralized visibility of OT activities, the network and entire organization become much more vulnerable. This lack of focus can contribute greatly to elevated OT security risks in any organization.
- **Clarity on Responsibilities:** who does what? Only 15% of OT professionals think that their CISO is responsible for OT security at their organization.[3] Not understanding where the responsibility lies is a significant problem for the organization.

status and evolution. Using the Enisa Return on Security Investment framework provides the board clear justifications towards security investments.

How to Convince the Board

Why Fortinet?

With over 20 years of experience in IT and OT cybersecurity, Fortinet deploys Defense-in-Depth with an integrated single-pane-of-glass management and analysis console, decreasing cyber risk, reducing the security burden on OT teams, as well as safeguarding production uptime and safety standards.



Issue #5

Regulation & Compliance: the depth of it

Staying compliant in the energy sector is no simple k. It takes time and an extensive knowledge of
the entire organization. To become certified after es a great deal of due diligence. To address
bal governments and organizations will take

s key. Consolidation in these standards across
ing to simplify the numerous regulations that

“Nea
nati
pas
to r
rans
pay
and
thr
in 2
num
thar

X

This is the list of some of the (current) regulations/frameworks facing the energy industry:

NIS Directive: This legislation aims to bolster cybersecurity across the EU.

ISA/IEC 62443: This framework is aimed at reducing current and future security vulnerabilities in industrial automation and control systems.

NIST Cyber Security Framework (CSF): This is a five-function approach to mitigating an organization’s cyber security risks. It’s usually combined with the following standards:

NIST 800-82: This guide provides a roadmap for securing industrial control systems.

ISO 27000 Series: These standards are focused on helping organizations strengthen their information security practices.

CIS Critical Security Controls: These are a set of actions that help organizations secure their data against cyberattack vectors.

NERC CIP: These standards are aimed at protecting national power grids, applicable on the North American Electricity grid.

TSA’s third directive (Security Directive Pipeline-2021-02C): Takes a performance-based approach to enhancing security, allowing operators to leverage new technologies and be more adaptive to changing environments. Applicable for the USA.

MITRE ATT&CK Framework for ICS: This is a globally accessible knowledge base of tactics and techniques used by cyber threat actors.

NISTIR 8374 (Draft): This guide is aimed at helping organizations manage their risks of ransomware attacks.

Other frameworks include:

GDPR: This legislation addresses data privacy and security in the EU.

Qatar ICS Security Standard: This standard underlines security controls for industrial automation systems in Qatar.

ENISA Guide to Protecting ICS (EU): This manual serves as a guideline to mitigate attacks on industrial control systems across the EU.

Regulations/Frameworks list ☰

Why Fortinet?

Fortinet aligns to these standards and guidelines. The deployment of a comprehensive, updated cybersecurity system with a mature governance framework must include a high level of IT/OT collaboration, as well as executive management support behind it all. The MITRE ATT&CK for ICS Framework is incorporated into Fortinet’s analysis and management products as well as providing a dedicated team to help support at every step of the way.