

STORMSHIELD

CYBERSECURITY & OPERATIONAL NETWORKS

How to begin factoring in risks for the industry of the future?

BAROMETER SURVEY PRODUCED IN COLLABORATION WITH L'USINE DIGITALE 2022

Contents

Key figures 04

01

WHETHER DIRECT OR INDIRECT, THE EFFECTS OF CYBER ATTACKS ARE PALPABLE

1.1 — What form do cyber attacks affecting industrial environments take? 06
1.2 — Cybersecurity's place in the world of industrial systems 07
1.3 — Perceptions are sometimes far from reality where risks are concerned 10
1.4 — Practical example: Connecting three factories in complete (cyber)security 13

02

SOLUTIONS ARE EVOLVING IN LINE WITH USES

2.1 — Deployment in keeping with the priorities of security projects 16
2.2 — Varied deployment according to the maturity of the industries concerned 19
2.3 — What are the solutions of tomorrow? 23
2.4 — Comparative interview — Toward an interoperable ecosystem 24
2.5 — Raising awareness among industrial companies: adaptation is the key 25

03

WHEN GOOD INTENTIONS MEET REALITY

3.1 — The shortage of specialised talent 28
3.2 — Securing the service chain 30
3.3 — Higher budgets to be allocated to industrial cybersecurity 32

Conclusion 33
Stormshield solutions 34
Bibliography/Sources and references 35

For three years running now, Stormshield and L'Usine Digitale have studied the digital transformation underway within companies and its impact on their IT security.

This year, we decided to offer an overview of cybersecurity practices in the operational environments of industrial companies.

Industrial IT (or OT for *Operational Technology*) covers all digital systems which allow for the automation of physical processes, while at the same time guaranteeing the satisfactory operation of a production line. These operational systems, which are increasingly connected to conventional IT systems (IT for *Information Technology*), require greater vigilance where cybersecurity is concerned.

For this reason, we begin by describing the cyber risks and threats facing the industrial sector. We then move on to describe the available solutions before looking at statements of intent and the reality out in the field as revealed by this study. Indeed, although they are using ever more connected equipment as part of the great adventure which is today Industry 4.0, some industrial companies seem to be unaware of or to underestimate the need to invest in cybersecurity to reduce these new attack surfaces in as far as possible.

As in previous years, we hope that this latest barometer survey will provide you with a constructive overview of the changes underway in the world of cybersecurity and particularly that of industrial environments.

Five key figures

51%

of respondents stated that they have suffered **at least one cyber attack on their operational network.**

32%

of respondents have introduced **OT network segmentation.**

45%

of respondents felt that **the need to take account of security issues can hinder** their operational projects.

27%

of respondents having already suffered a cyber attack **saw their production stopped or disrupted.**

39%

of respondents have deployed **solutions to protect IT/OT interconnections.**

These figures bear out what we are seeing in the field: cyber security measures are now being put in place. For example, it is still rare to have a secure IT/OT Interface, which makes industrial systems particularly vulnerable to the bounce (intentional) or even edge effects (accidental) of cyber attacks on the IT system (information technology system).

Thaïs L., Senior auditor for a French pure-player in the cybersecurity field

01

WHETHER DIRECT OR INDIRECT, THE EFFECTS OF CYBER ATTACKS ARE PALPABLE

1.1 — What form do cyber attacks affecting industrial environments take? 06
1.2 — Cybersecurity's place in the world of industrial systems 07
1.3 — Perceptions are sometimes far from reality where risks are concerned 10
1.4 — Practical example: Connecting three factories in complete (cyber)security 13

1.1.

What form do cyber attacks affecting industrial environments take?

With the emergence of the concept of the "industry the future", we are seeing increasing maturity in the cybersecurity field. This now concerns the protection of the industrial system, viewed as an overall system. A system which encompasses the industrial IT system (IIT, built around the ever present SCADA, ICS/DCS and APIs), as well as the machines, software, workstations and different network equipment.

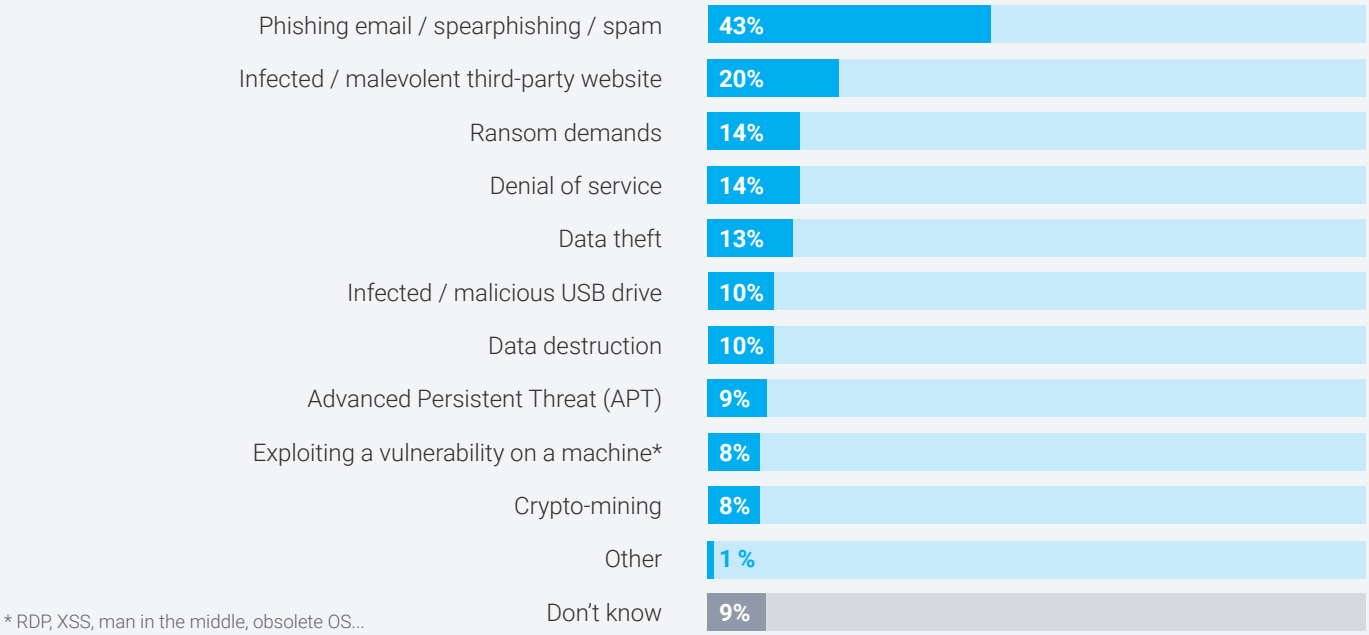
Consequently, **51%** of those interviewed stated that they have suffered at least one cyber attack targeting the operational network. The recent attacks on the ports in northern Europe raise the spectre of this figure rising further.

Regarding the origin of the cyber attacks, most of them affecting production equipment find their way in through the IT systems. There's obviously nothing new there, because the interconnection of the conventional IT and operational IT systems is increasing, which presents industry with a major risk.

51%

of respondents stated that they have suffered at least one cyber attack targeting their operational network

WHAT SORT OF ATTACKS ARE WE TALKING ABOUT?



* RDP, XSS, man in the middle, obsolete OS...

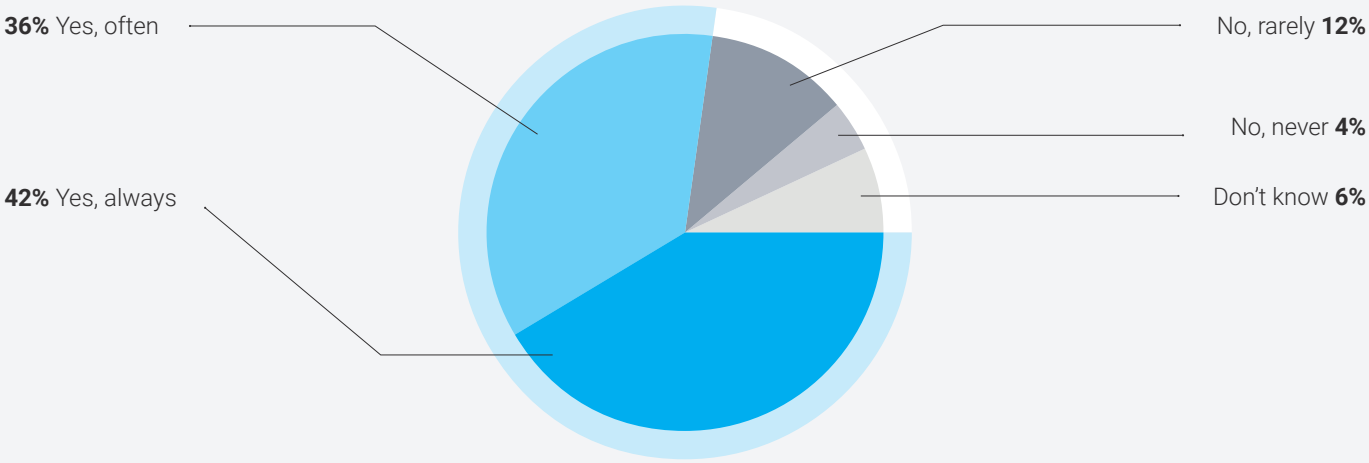
1.2.

Cybersecurity's place in the world of industrial systems

The convergence between IT and OT has already been a reality for several years at both a technical and organisational level. These two environments, using technologies which were once very different and isolated are today interconnected. And the cyber management principles in the world of IT must adapt to the industrial environment, meeting a specific need for security and risk management.

In this industrial environment, in which availability remains the priority, the cybersecurity aspect is taken into consideration upstream of most projects (**78%**).

IS CYBERSECURITY INCORPORATED UPSTREAM OF PROJECTS RELATED TO YOUR OPERATIONAL ENVIRONMENT?



78% YES / NO 16%

The interconnection of IT and OT is a reality, but its effects have not yet been fully taken on board. However, the consequences of a cyber attack in such environments can be far more violent than a typical IT attack.

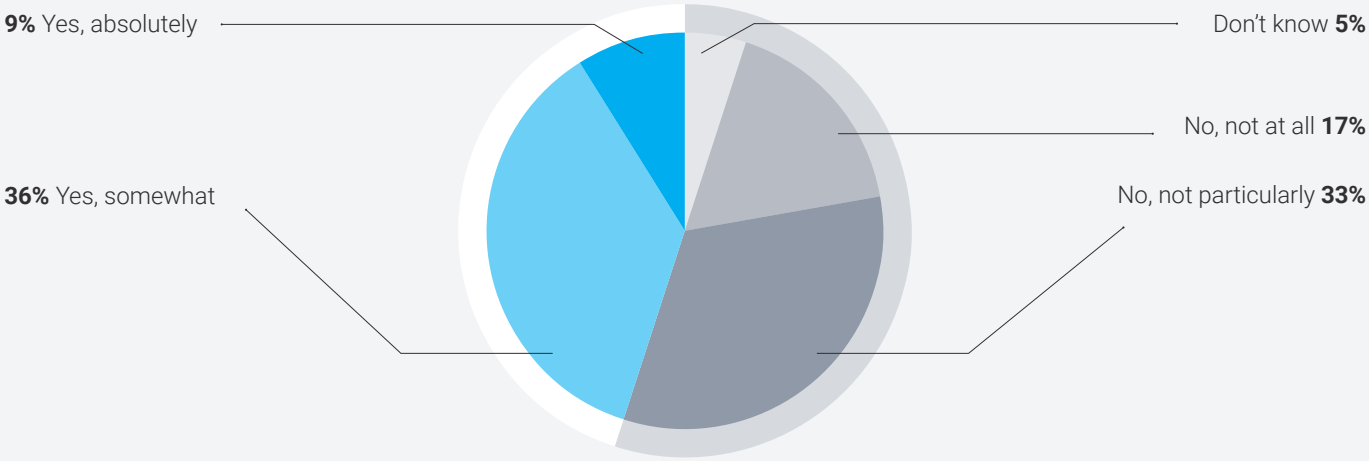
Marc Fromager, VP Industrial Automation & End Users, Schneider Electric France

However, almost half of those surveyed said that the need to take account of security issues can hinder their operational projects.

45%

of respondents stated that the need to take account of security issues is still seen as hindering their operational projects

IN YOUR VIEW, DOES THE NEED TO TAKE ACCOUNT OF SECURITY ISSUES HINDER YOUR OPERATIONAL PROJECTS?



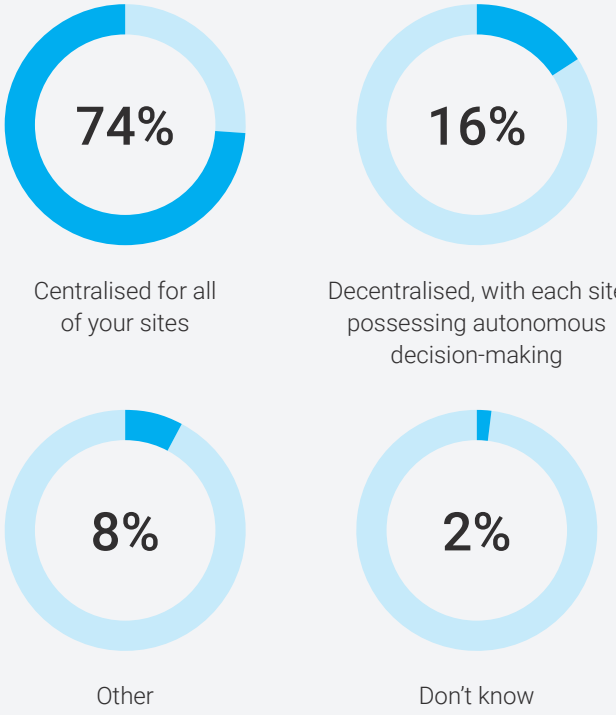
45% YES / NO 50%

As cybersecurity experts, it's our job to adapt to operational constraints, to find easy-to-deploy solutions such as pass-based authentication rather than requiring users to remember a different password for each machine.

Thaïs L., Senior auditor for a French pure-player in the cybersecurity field

Regarding governance, almost **3 out of 4 respondents** opted for a centralised industrial cybersecurity policy. This organisational structure makes it possible to standardise security for all industrial IT systems while at the same time retaining some room for manoeuvre locally and meeting the specific needs of each site. This centralised approach to security management provides a benchmark to guarantee a minimum level of security based on the CISOs or dedicated on-site OT coordinators.

IN YOUR OPERATIONAL ENVIRONMENTS, IS CYBERSECURITY GOVERNANCE:



IT and OT are still two different worlds. But we are moving towards shared governance and single teams comprised of experts with twofold cyber and industrial skills.

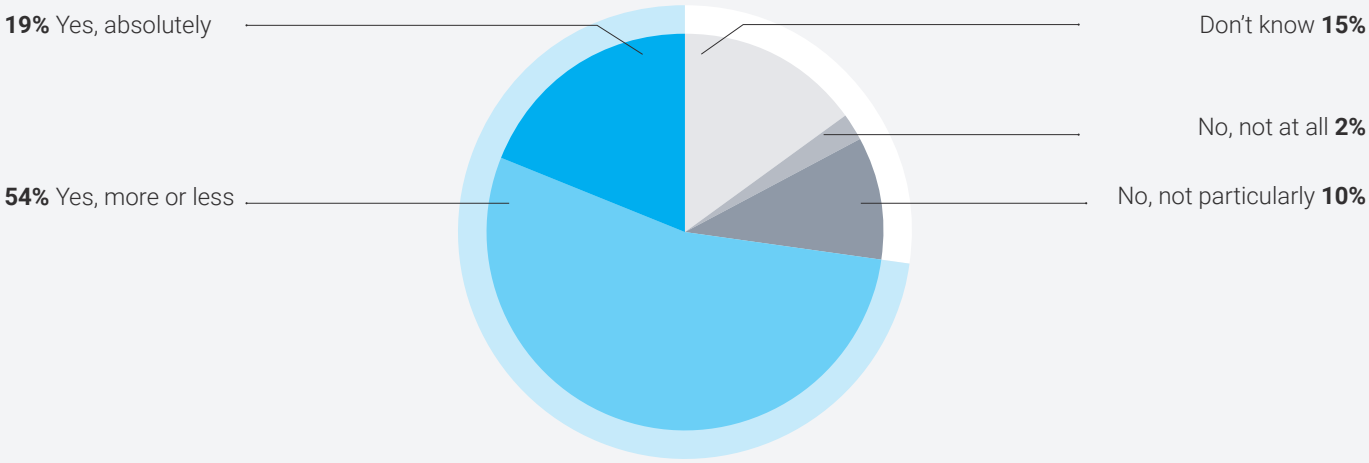
Rodolphe de Beaufort, Assistant General Manager of GIMELEC and Organiser of the CyberOT Club

1.3.

Perceptions are sometimes far from reality where risks are concerned

From a technical viewpoint, the respondents appeared to be satisfied with the solutions at their disposal. Indeed, **73%** of them considered that the existing technologies meet all of their cybersecurity challenges. It's important to highlight that according to how these technical resources are used, the true protection level can vary a great deal. The challenge is to deploy the right tools in the right places and then get them working correctly on a daily basis.

DO EXISTING TECHNOLOGIES MEET ALL OF YOUR CYBERSECURITY CHALLENGES?

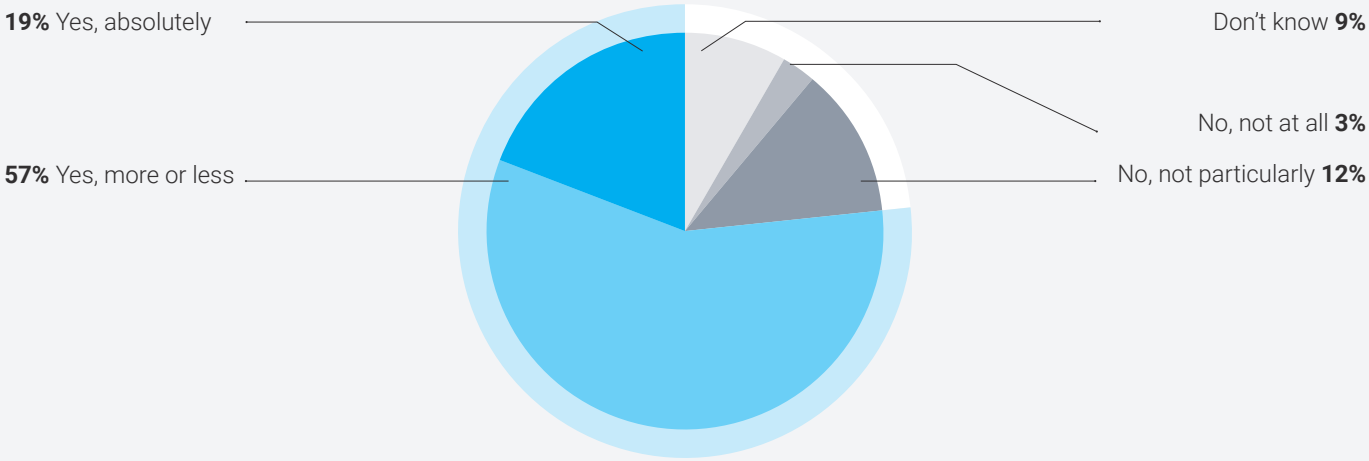


73% YES / NO 12%

The survey also showed that a surprising proportion of decision-makers have a great deal of confidence in the cybersecurity aspects of their industrial systems (**76%**), even during the maintenance phases (**70%**).

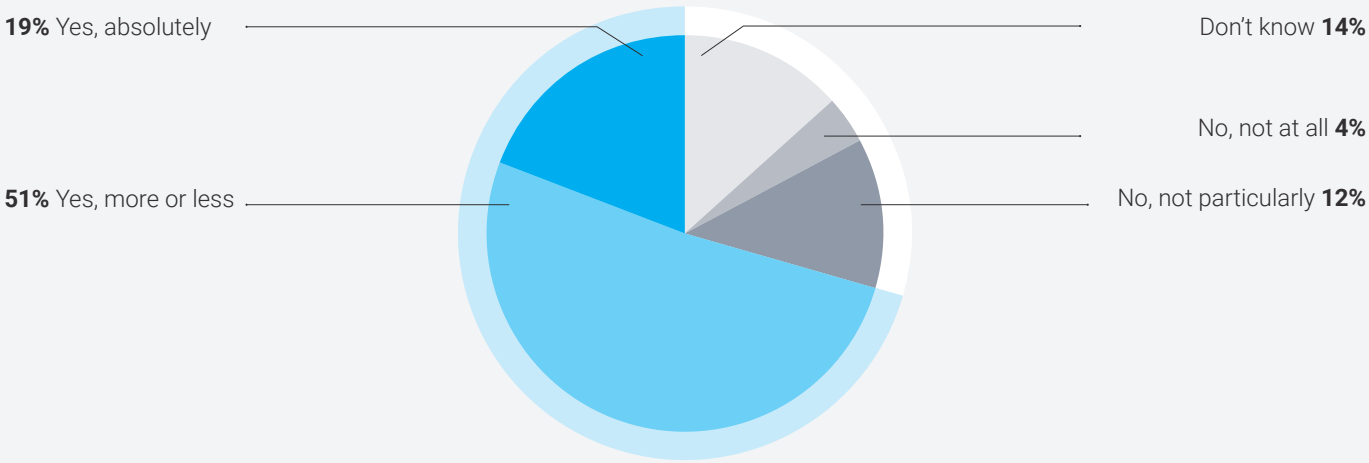
When we look at the figures more closely, the most confident among them are the senior management, the operations and R&D departments (**85%**), the CIOs (**76%**), the production or maintenance departments (**75%**) and the digital strategy departments (**69%**). This proportion decreases for staff from the security-safety departments (**56%**) and the risk management departments (**50%**).

WOULD YOU SAY THAT YOUR COMPANY IS SUFFICIENTLY PROTECTED AS REGARDS CYBERSECURITY IN ITS OPERATIONAL ENVIRONMENT?



76% YES / NO 15%

WOULD YOU SAY THAT YOUR COMPANY IS SUFFICIENTLY PROTECTED AS REGARDS CYBERSECURITY DURING THE MAINTENANCE PHASES?



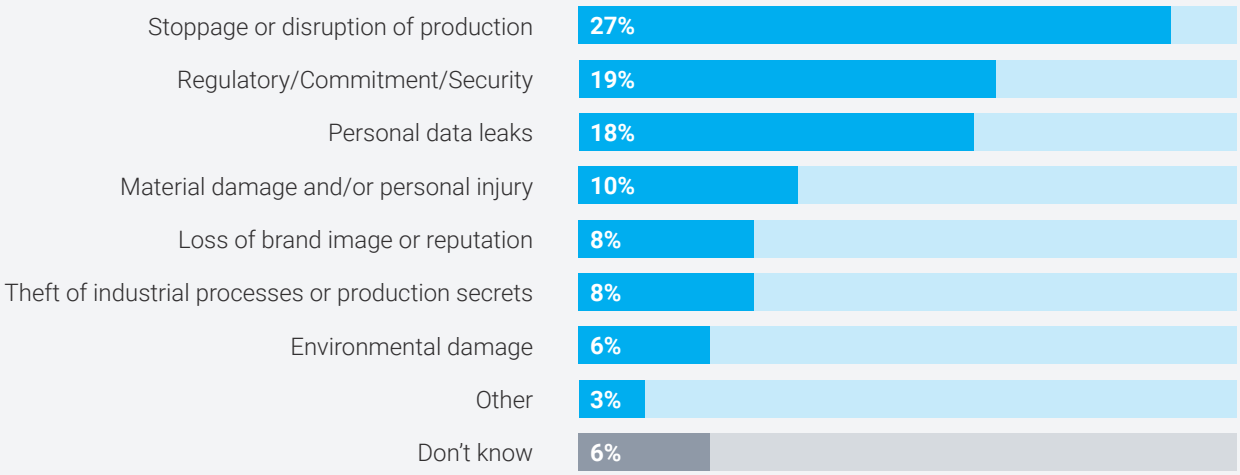
70% YES / NO 16%

However, cyber criminals are already making the most of the undeniable increase in the attack surface of industrial systems: among the respondents having suffered cyber attacks, **27%** reported that this led to the stoppage or disruption of production .

27%

stated that the cyber attacks they suffered led to a stoppage or disruption of production

WHAT HAVE BEEN THE CONSEQUENCES OF THE CYBER ATTACKS?



There are plenty of examples and they are attracting increasing media coverage. In March 2019, the Norwegian aluminium specialist Norsk Hydro suffered a ransomware attack (LockerGoga) which directly affected its industrial IT system. After being obliged to disconnect its different sites and factories, the company estimated the impact of this cyber attack at 46 million euros, without paying the ransom demanded. At the time, many media outlets praised the group for its crisis communications. Since then, the list of companies suffering cyber attacks has constantly grown and the extremely transparent position adopted by Norsk Hydro is hailed as an example.

So, how do we explain the apparent difference between industrial companies' sense of security and their actual protection levels? It seems that a certain lack of risk awareness still persists, with such risks being better understood by cybersecurity experts than by industrial managers. Being closer to the operational aspects of the business, the latter have the task of ensuring that processes work properly but do not fully appreciate the cyber aspects. These two spheres with their complementary skills therefore need to be brought together.

Risk awareness is still a work in progress for some industrial companies who cannot imagine that their industry could become a target.

Thaïs L, Senior auditor for a French pure player in the cybersecurity field

PRACTICAL EXAMPLE

Connecting 3 factories in complete (cyber) security

One of Stormshield's industrial clients was looking to interconnect three factories in France. With each possessing more than a hundred items of equipment, the cybersecurity aspect of the project was vital in order to avoid any possible infection by malware, the loss of control of a machine to an attacker, the theft of critical data or industrial espionage, etc.

Stormshield identified the need to secure the activity-specific data from the manufacturing execution system (MES) and the logging servers while proposing secure access.

PROTECTING ENTRY POINTS AND INTERCONNECTIONS

The Stormshield Network Security solution was chosen to guarantee the security of the company's IT systems. An SN2100 cluster was introduced for each of the three sites to optimise the segmentation and separation of the OT networks of each site from the rest of the IT system, where all the industrial data related to operations is uploaded and centralised.

Some ten SNi40 firewalls, specially designed to protect PLCs, were also deployed to provide security closer to the equipment itself.

THE ADVANTAGE OFFERED BY THE STORMSHIELD SOLUTION

These boxes also allow IP address plans to be standardised via the "Network Address Translation" function (NAT), in particular for the so-called "approved" machine islands supplied by external equipment manufacturers which have their own IP addresses which cannot be modified to maintain the manufacturer's warranty. SNi40 firewalls can translate the equipment address at the Internet connection gateway between the internal address of the machine and the IP address of the gateway, which allows a PLC to be seamlessly integrated into the client's addressing scheme. By deploying Stormshield equipment, the customer was also able to improve the visibility of its industrial information system thanks to the "Intrusion Detection System" (IDS) mechanism, which can detect malicious traffic and raise an alarm.

THE BENEFITS OF THE SOLUTION

- a easy installation thanks to transparent network integration functions, making it possible to rapidly adapt to the activity-specific and operational context,
- a application plug-in technology for maximum protection against known threats and zero-day attacks,
- a protocol inspection capabilities to ensure compliance with industrial protocols to avoid attacks and human error,
- a a small equipment footprint on latency in the industrial network,
- a a single software solution for a one-step administration process, regardless of the protection domain (OT or IT).

MAKING FULL USE OF ALL INDUSTRIAL DATA

Fully satisfied with the interconnection of its IT and OT networks, this major industrial group continues to place its trust in Stormshield to equip all our European sites over the coming months, and its worldwide sites in the longer term.

02

SOLUTIONS ARE EVOLVING IN LINE WITH USES

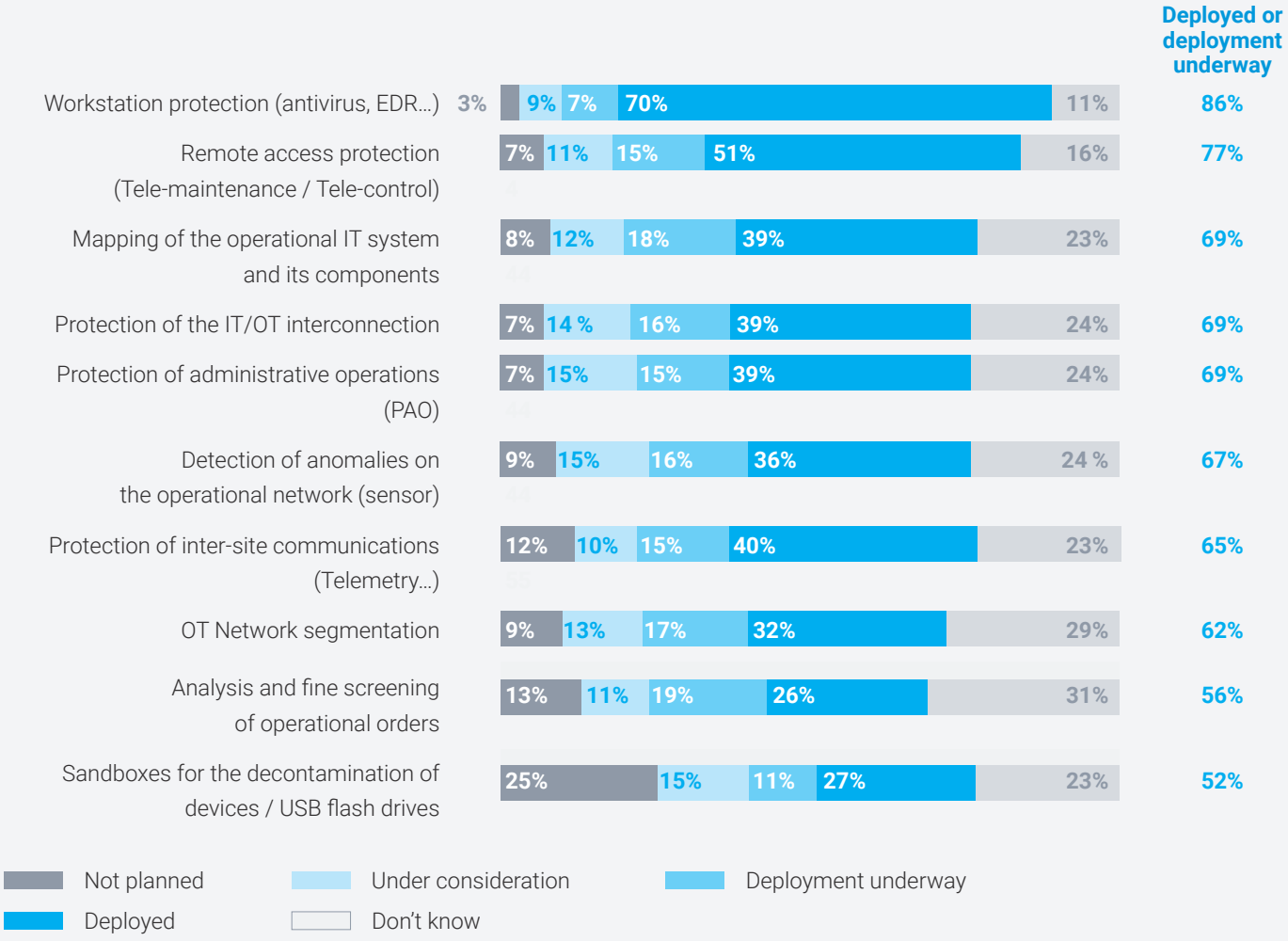
2.1 — Deployment in keeping with the priorities of security projects **16**
2.2 — Varied deployment according to the maturity of the industries concerned **19**
2.3 — What are the solutions of tomorrow? **23**
2.4 — Comparative interview — Toward an interoperable ecosystem **24**
2.5 — Raising awareness among industrial companies: adaptation is the key **25**

2.1.

Deployment in keeping with the priorities of security projects

Among the first solutions which come to mind, the **protection of workstations** via an antivirus or EDR is widely deployed in the operational environments of those surveyed (**70%**). At the same time, **52%** of the respondents stated that they use or are thinking about

WHICH PROTECTIVE MEASURES ARE USED OR WILL BE USED IN YOUR COMPANY TO SECURE YOUR OPERATIONAL ENVIRONMENTS?

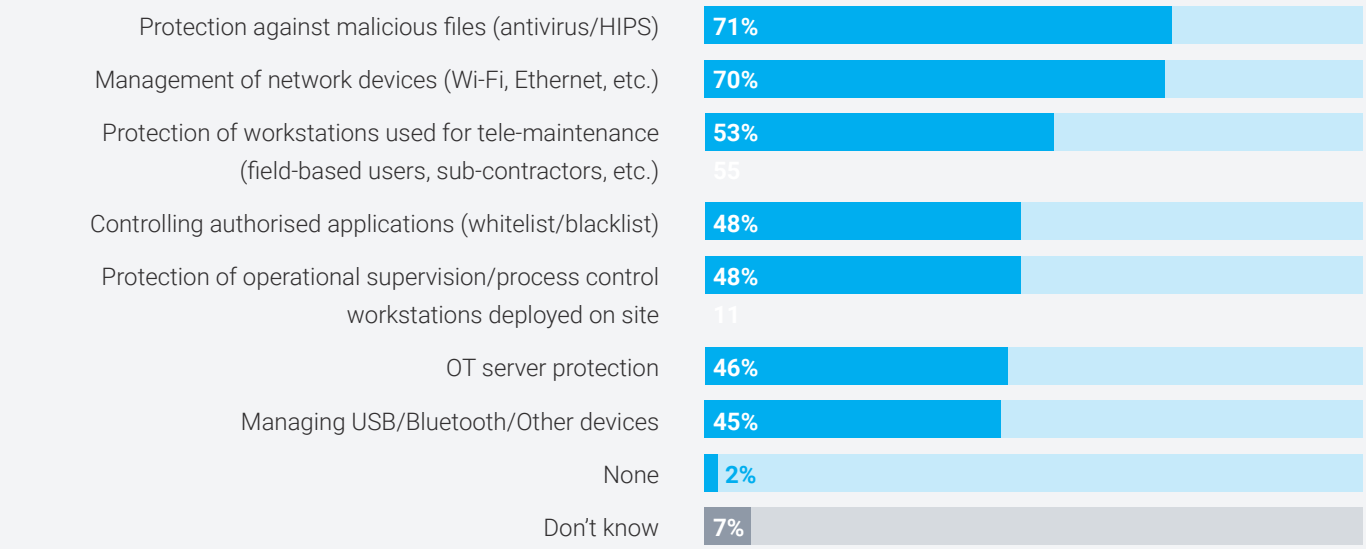


With the arrival of the IoT and supervision tablets in the factories, several respondents also mentioned the management of network devices (Wi-Fi, Ethernet, USB and Bluetooth) as an operational perimeter needing to be secured (**70%** and **45%** respectively).

Remote access protection is in place for half of them. This figure is partly explained by the increased use of tele-maintenance, particular during the Covid-19 pandemic. Though more practical, these access points unfortunately aren't always identified, creating new doorways into the system, which must be secured at all costs.

The **mapping** of the entire OT environment is also a prerequisite to securing it, but this is something which has only been undertaken at **39%** of respondents' firms.

ACROSS WHICH FUNCTIONAL PERIMETER HAS YOUR COMPANY DEPLOYED OR PLANS TO DEPLOY WORKSTATION PROTECTION SOLUTIONS?



The sensors and the mapping make it possible to identify the equipment actually present on the network, and to spot vulnerabilities or configuration errors. With this information, it's possible to focus priorities for other solutions and to undertake the right decisions when it comes to allocating budgets and maintenance slots.

Vincent Dély, Nozomi Networks

The same proportion of respondents stated that they have deployed protection solutions covering IT/OT interconnection and administrative operations (PAO). The improvement of **authentication** is one of the major areas requiring work for these industrial organisations which, in the main, have no Active Directory and whose management of accesses and privileges is relatively ineffective.

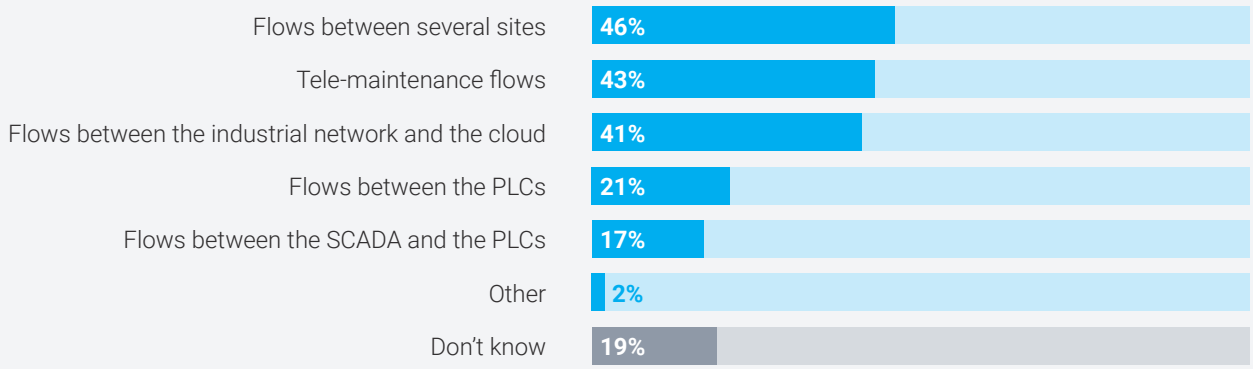
For its part, the **protected inter-site communication** is in place at the firms of **40%** of the respondents and also presents major challenges, as seen by the cyber attack suffered by Honda in 2020: several of its production sites worldwide were blocked by a ransomware attack. The carmaker had to ensure that its quality control systems had not been compromised before resuming production.

Just 32%

of respondents stated that they have deployed OT network segmentation

These inter-site flows were mentioned among the **operational flows secured or needing to be secured** by **46%** of the respondents. Only 17% of them mentioned flows between the SCADA and the PLCs, which are probably not seen as a priority in the security process.

WHICH OPERATIONAL FLOWS HAVE YOU SECURED OR DO YOU ENVISAGE SECURING?



Solutions such as the **analysis and screening of operational commands** are still less common – despite the advanced security capabilities they offer. The latter require a high degree of cyber maturity on the part of the industries concerned. They involve going into the detail of the industrial process and that means having already put in place other, more urgent, protective measures.

Ultimately, guaranteeing cybersecurity for operational environments is a long-term work in progress and the figures we received bear witness to the state of progress with the deployment of protection in these environments. For example, **OT network segmentation** is something which takes time, particularly if it involves several industrial sites, as it requires the deployment of a gateway (DMZ) between the corporate network (IT) and the operational side (OT network). This could explain why **68%** of respondents have not yet deployed it. It should also be noted that the notion of prioritisation in the deployment of industrial cybersecurity is all the more important since the intervention timeslots are reduced, as production cannot be stopped for very long or very often.

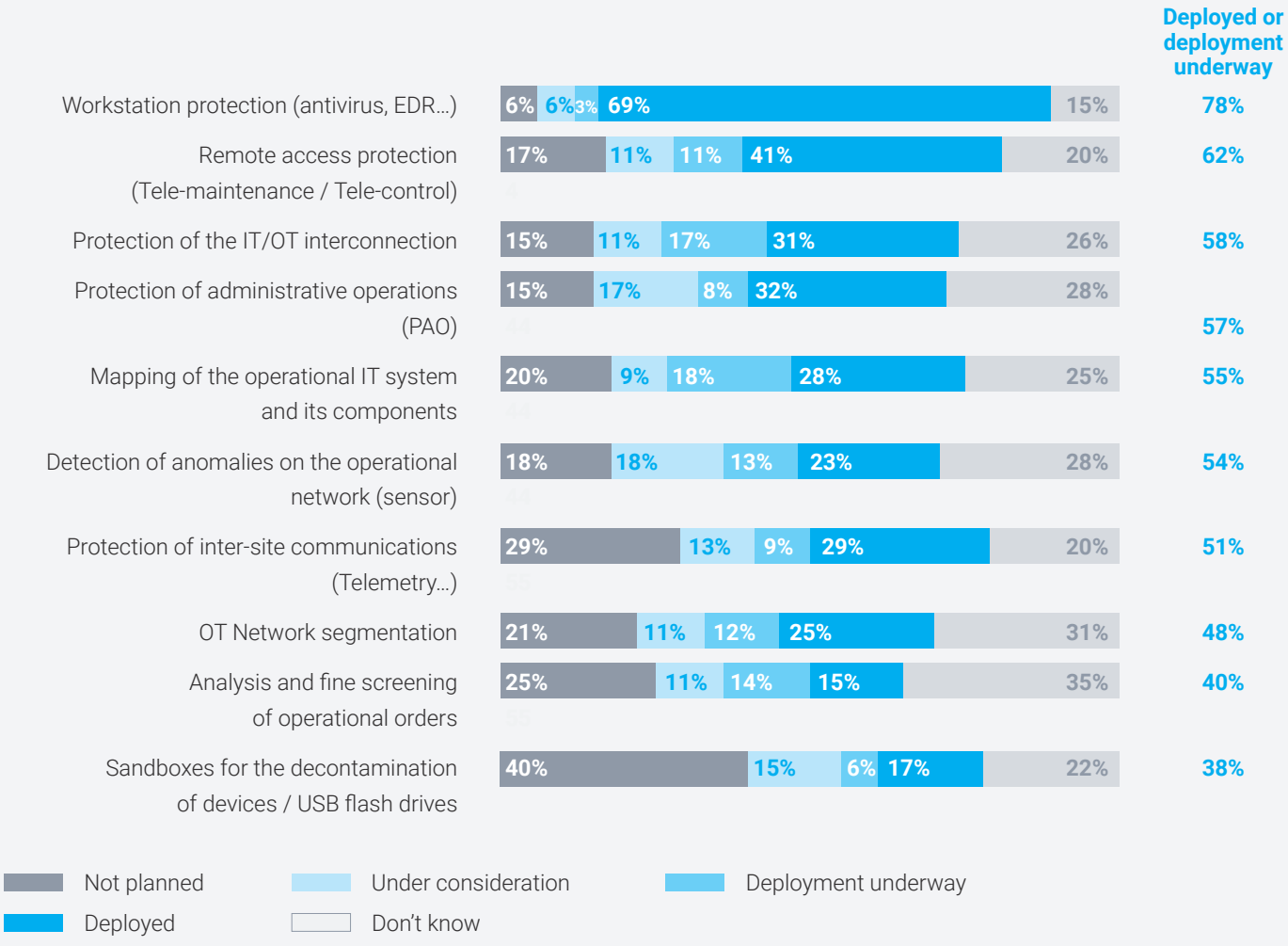
2.2.

Varied deployment according to the maturity of the industries concerned

The number and type of cybersecurity solutions deployed varies according to the industry type. Very small businesses and small-to-medium-size businesses are those which declare the lowest level of investment in cybersecurity, with intermediate-sized businesses being those envisaging the deployment of more protection solutions while large businesses appear to already be equipped with them.

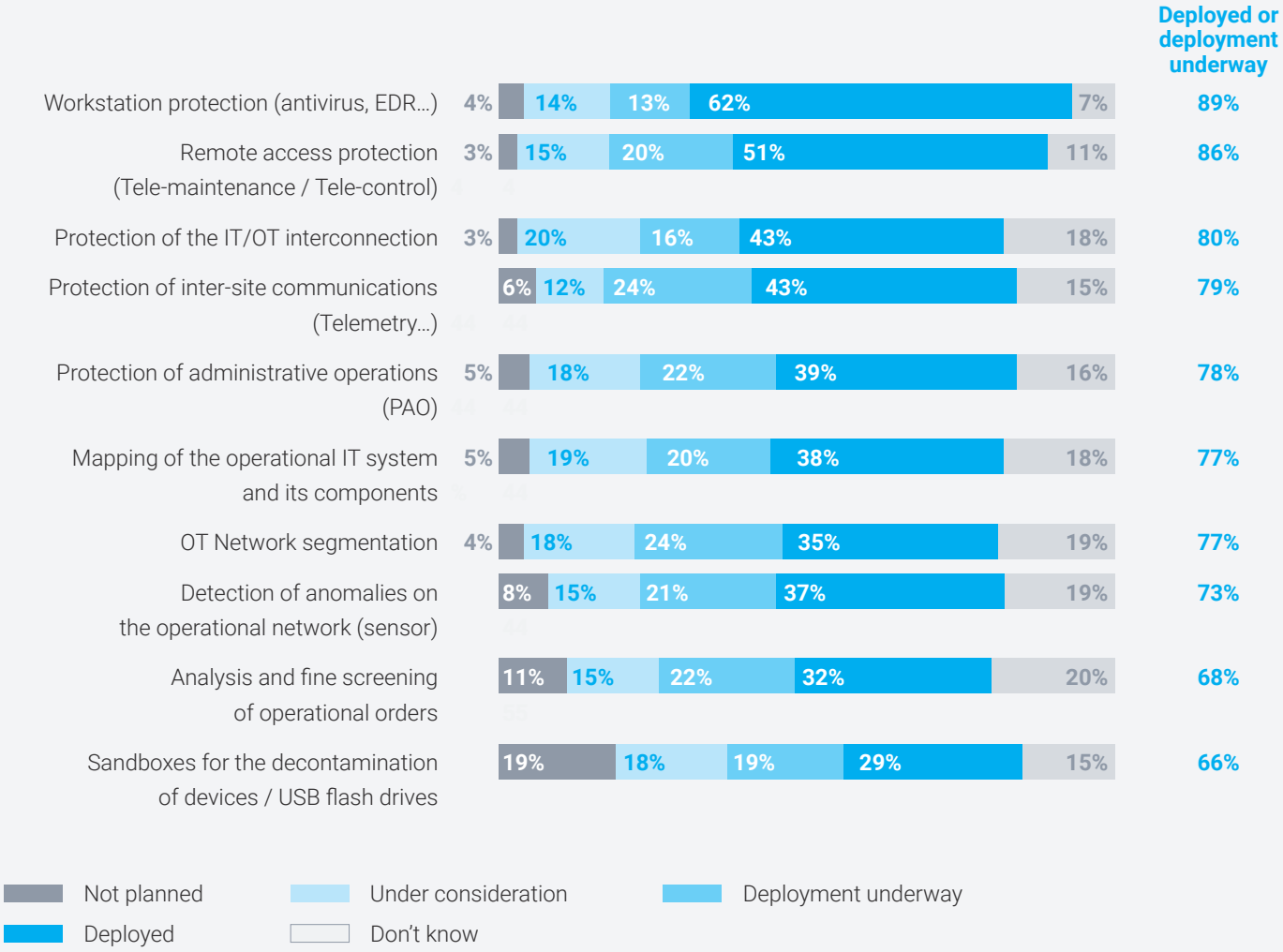
SPOTLIGHT ON VERY SMALL AND SMALL-TO-MEDIUM BUSINESSES

WHICH PROTECTIVE MEASURES ARE USED OR WILL BE USED IN YOUR COMPANY TO SECURE YOUR OPERATIONAL ENVIRONMENTS?



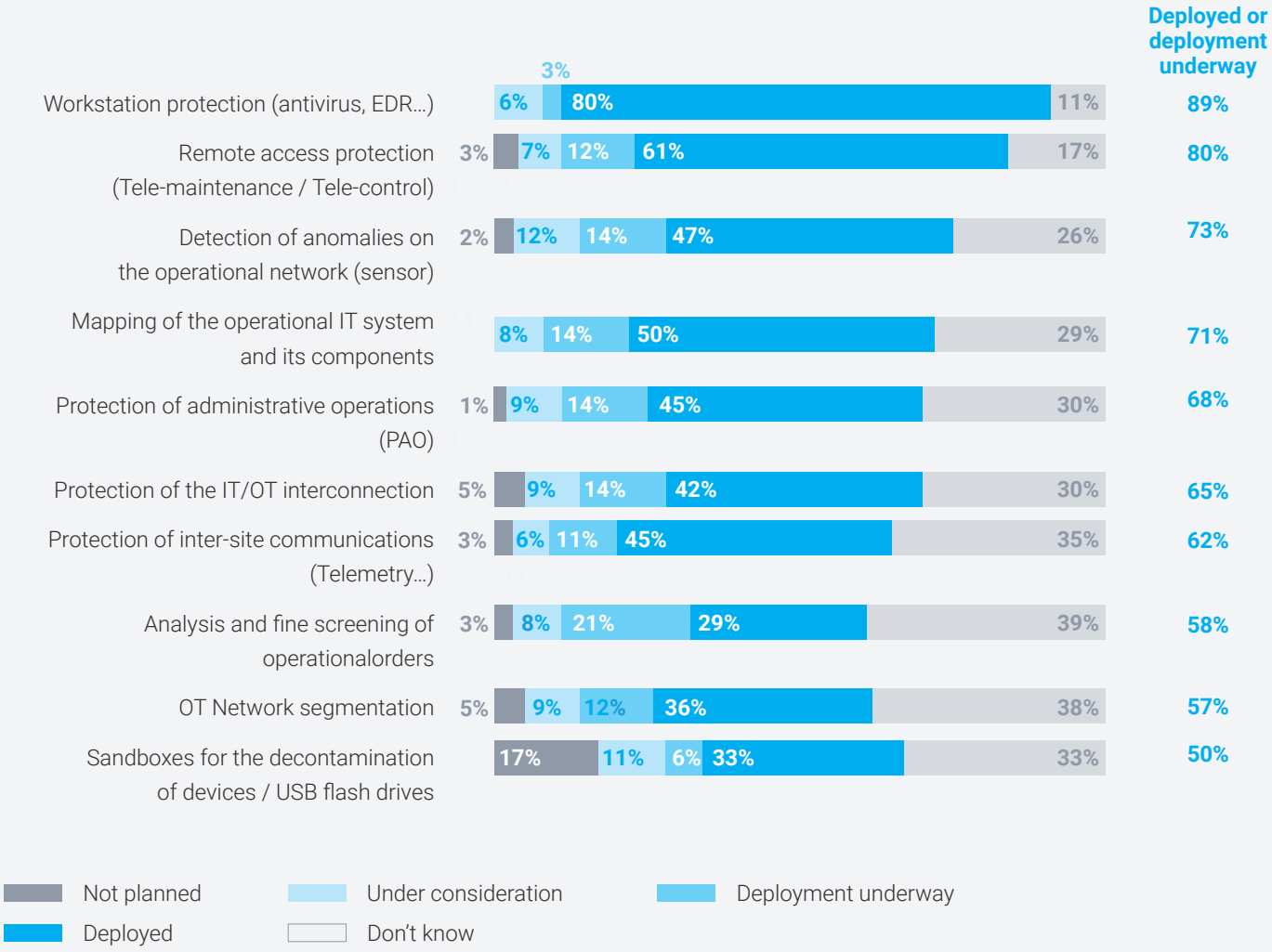
SPOTLIGHT ON INTERMEDIATE-SIZED BUSINESSES

WHICH PROTECTIVE MEASURES ARE USED OR WILL BE USED IN YOUR COMPANY TO SECURE YOUR OPERATIONAL ENVIRONMENTS?



SPOTLIGHT ON MAJOR COMPANIES

WHICH PROTECTIVE MEASURES ARE USED OR WILL BE USED IN YOUR COMPANY TO SECURE YOUR OPERATIONAL ENVIRONMENTS?



This varied situation is explained by widely differing resources available to major groups and small businesses, but there's more too. As a result of their activities, which may be considered as critical, some industrial organisations are subject to extensive regulatory obligations while others are left free to act based on their own assessment of the risks they face. At least for the time being.



The regulations currently target so-called critical industries such as energy, transport or chemicals. Within 2 to 5 years, all industrial sectors will be concerned.

Rodolphe de Beaufort, Assistant General Manager of GIMELEC and Organiser of the CyberOT Club

The advances achieved in the industrial cybersecurity field by the major groups are also due to the improved security of their conventional IT systems. They can now focus on protecting their operational environments.

2.3.

What are the solutions of tomorrow?

In addition to the solutions already discussed, such as the mapping of systems or securing accesses, the respondents also mentioned various means for better protecting their operational environments. Among these we find the old favourites, such as improved awareness building for employees, regularly changing passwords, daily off-site backups, the introduction of firewalls or data breach detection.

Two major trends are also emerging, with:

→ the development of **new hardware components** for the products. This new generation of PLCs, sensors and protocols integrates (and will integrate) security natively.

→ the deployment of **cloud solutions** , over and above cybersecurity. Some industries are envisaging deploying cloud infrastructures to boost their computing power. This migration makes it possible to process larger volumes of data, including production data uploaded from the IoT sensors and required for the development of predictive maintenance for example. The use of the cloud also makes it possible to optimise infrastructure and productivity by displacing non-essential aspects to focus instead on operational excellence. New cybersecurity solutions are making their appearance, to secure this new perimeter.

As an example, Jean-Yves Poichotte, Cybersecurity Director for the Sanofi group, recently declared that Sanofi's objective was to eventually have **50%** of its infrastructure in the cloud. At the other end of the strategic spectrum, some respondents stated that they were favourable to bringing the system in-house.

Schneider Electric's R&D teams have adopted a "cybersecurity by design" approach: cybersecurity is baked into all of our connected or connectable products from the design stage, before the different functions have even been developed.

Marc Fromager, VP Industrial Automation & End Users, Schneider Electric France

COMPARATIVE INTERVIEW

Toward an interoperable ecosystem

With Vincent Nicaise, Stormshield Industrial Partnerships and Ecosystem Manager, and Khobeib Ben Boubaker, Head of Industrial Security Business Line Stormshield

BETTER PROTECTION THROUGH COMMUNICATION

Khobeib Ben Boubaker — Interoperability, i.e. the ability of systems to operate together, has long existed in the IT field. Where OT is concerned, this is still in the process of taking shape.

Vincent Nicaise — When we talk about interoperable industrial cybersecurity solutions, this includes both 'pure OT' and OT/IT solutions: here I'm thinking for example of firewalls deployed in an operational environment which upload information such as security logs in a SOC IT.

PROMOTING THE PRINCIPLE OF IN-DEPTH DEFENCE

Vincent Nicaise — Interoperability makes it possible to facilitate management and improve the efficiency of a technical environment comprised of the best solutions in each field. This multi-specialist or best-of-breed approach promotes the application of the in-depth defence principle to IT systems, whether these are conventional or industrial.

Khobeib Ben Boubaker — Naturally, a good level of cooperation between the best publishers in the cybersecurity field is very important. But the desire for interoperability must also be supported by the whole ecosystem, beginning with the industrial companies themselves, which must accept data sharing.

A SUCCESSFUL EXAMPLE OF COOPERATION

Vincent Nicaise — We have set up a technology partnership with the industrial sensor supplier Nozomi Networks. These sensors provide an inventory along with the advanced detection of cyber threats in industrial environments, but do not make it possible to directly respond to the incidents detected. Integration with a Stormshield firewall provides this capacity. When the Nozomi Networks sensor detects a vulnerability in the network, it automatically issues a firewall rule to neutralise the attack or reduce its impact. The sharing of the status of the equipment identified on the network between the two solutions also makes it easier to manage security rules.

Khobeib Ben Boubaker — There's a natural logic behind the combination of our complementary, CSPN certified solutions: they make it possible for the industrial world to embrace active cyber-surveillance!

2.4.

Raising awareness among industrial companies: adaptation is the key

Awareness building is the leading means used to tackle the challenges of cybersecurity in operational environments. It was mentioned by **62%** of respondents.

WHICH MEANS HAVE BEEN EMPLOYED BY YOUR COMPANY TO TACKLE THE CHALLENGES OF CYBERSECURITY IN YOUR OPERATIONAL ENVIRONMENTS?

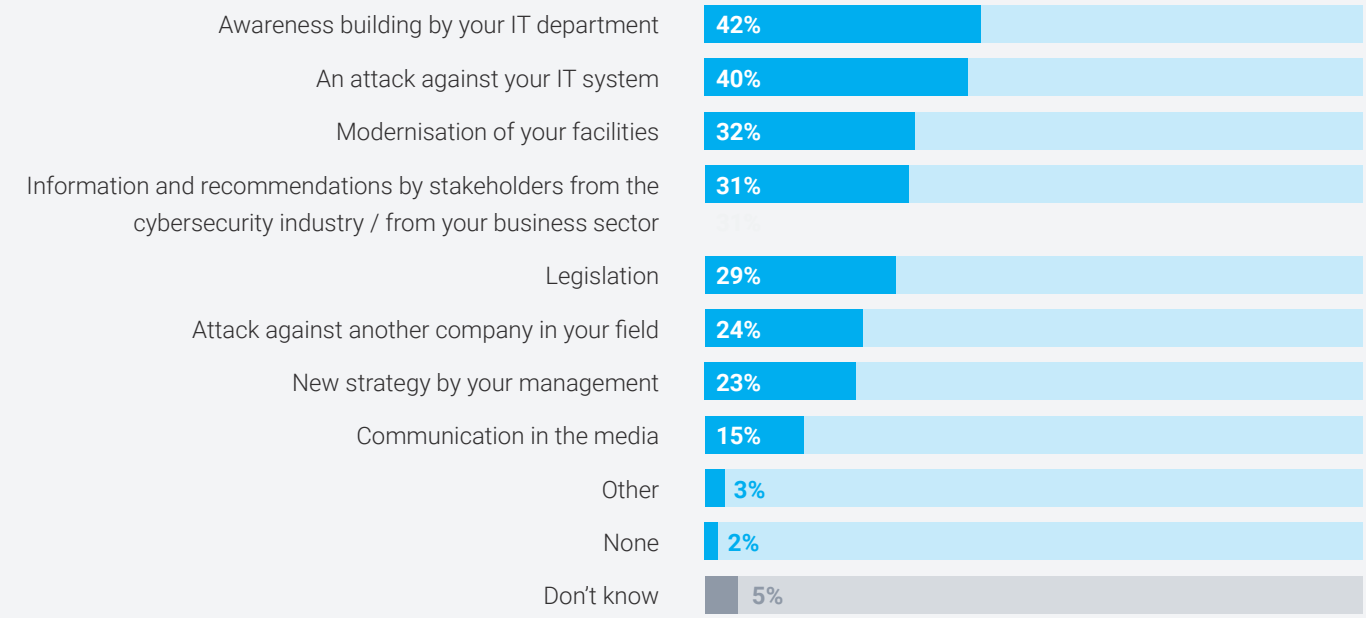


For industrial crew members to be made aware of cybersecurity in their personal use of IT resources, pragmatic training activities adapted to their context are vital.

The awareness building work must also extend to the industrial company's whole logistics chain. Until other solutions such as secure components are more mature, this remains one of the most effective means of dealing with the cyber problem.

Awareness building is also mentioned as a factor in triggering the introduction of cybersecurity solutions in operational environments by **42%** of respondents.

WHICH FACTORS HAVE TRIGGERED THE INTRODUCTION OF CYBERSECURITY SOLUTIONS IN YOUR OPERATIONAL ENVIRONMENT?



The incorporation of industrial cybersecurity is still fairly new and reactive. We are often asked to perform post-recovery audits following an attack, and more rarely preventive ones.

Thaïs L., Senior auditor for a French pure-player in the cybersecurity field

03

WHEN GOOD INTENTIONS MEET REALITY

3.1 — The shortage of specialised talent **28**
3.2 — Securing the service chain **30**
3.3 — Higher budgets to be allocated to industrial cybersecurity **32**

3.1.

The shortage of specialised talent

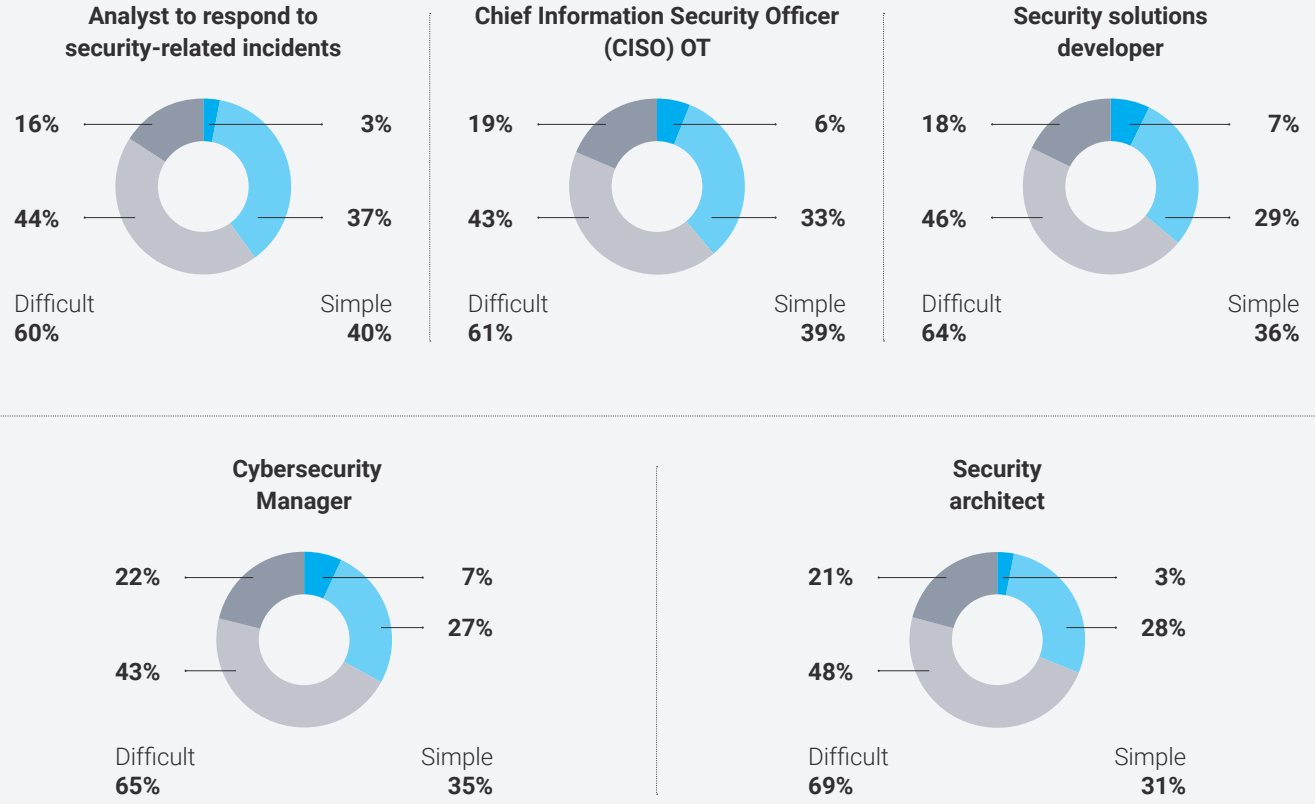
According to Capital, cybersecurity consultants are listed among the 8 "new" highly sought-after professions in industry. Our study highlights extremely significant recruitment difficulties for the various jobs related to industrial cybersecurity. Between **60%** and **70%** of respondents considered that these positions are difficult or even very difficult to fill. A figure which is hardly surprising when considering the situation in the cyber employment market in general.

Nevertheless, industrial cybersecurity needs specialists as its priorities are very different: the management of accesses, security... everything must be tailored to maintain availability and productivity.

70%

Up to 70% of respondents stated that cybersecurity positions are difficult or even very difficult to fill

IN YOUR OPERATIONAL ENVIRONMENTS, IN YOUR EXPERIENCE HAS THE RECRUITMENT OF PEOPLE FOR THESE CYBERSECURITY POSITIONS BEEN SIMPLE OR DIFFICULT?





To secure an infrastructure comprised of PLCs, it's important to understand the industrial process.

Marc Fromager, VP Industrial Automation & End Users, Schneider Electric France

The engineering schools don't yet offer academic training designed to match these dual-skill job profiles. Under such conditions, learning is chiefly conducted on-the-job and/or via training modules proposed by some stakeholders in the sector such as Schneider Electric.

So is it better to upgrade the skills of automation engineers, who are experts in the OT field, or to train IT cyber experts in OT matters? The debate is ongoing and also points to a third option, that of collaboration between the cyber and occupational teams. This is vital to keep pace with an industrial cybersecurity market growing by more than **7%** annually.

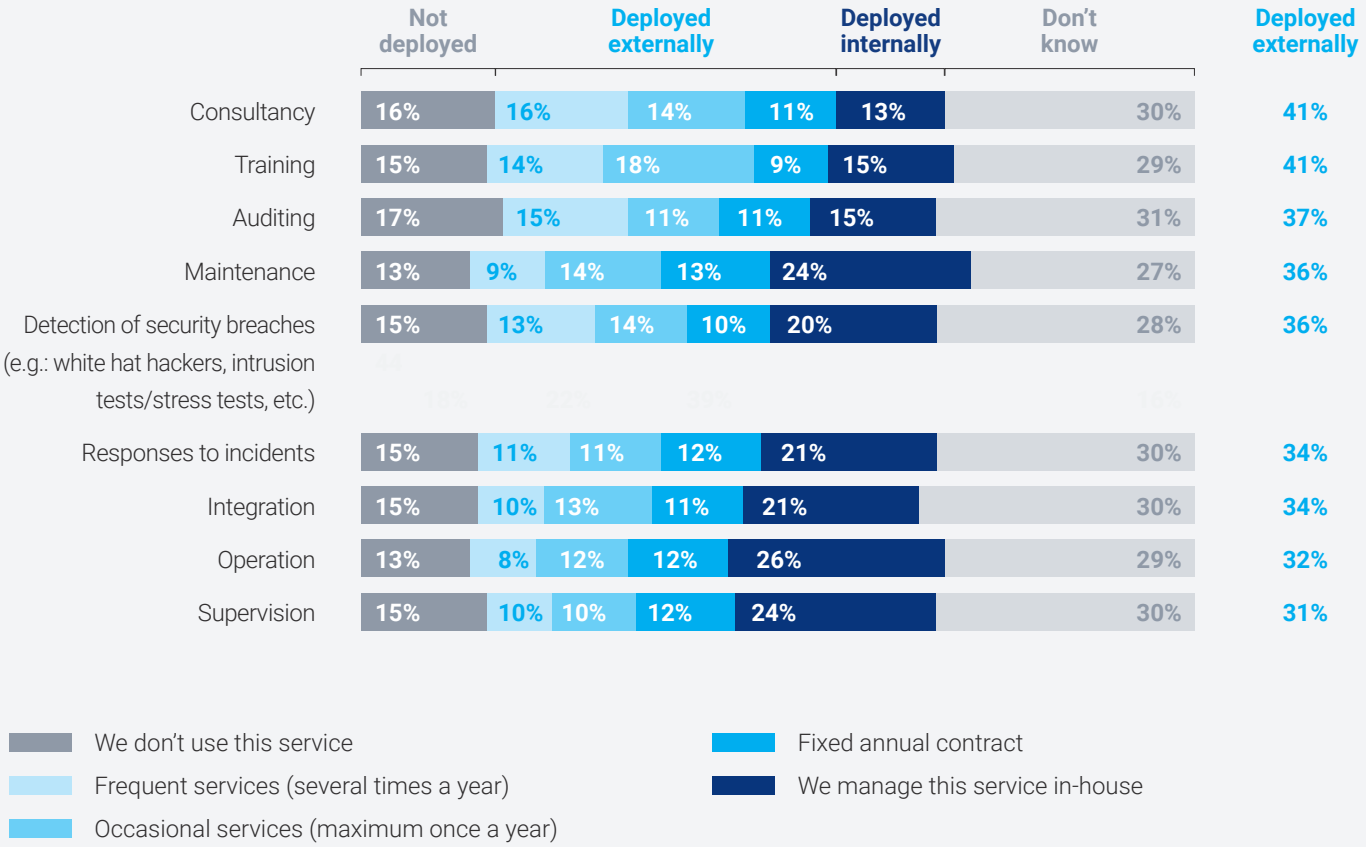
3.2.

Securing the service chain

The supply and service chains for industrial companies have always involved many stakeholders. To this long list, we must now add cybersecurity companies as **41%** of respondents use the services of specialised consultancy companies in this field, for example.

Whether we're talking about a response to an incident (**34%**), integration (**34%**), operation (**31%**) or supervision (**32%**), almost a third of those surveyed also use one or several outside companies. And they do so at least once a year. Almost **4 respondents out of 10** outsource maintenance, auditing or security breach detection activities.

HOW OFTEN DO YOU USE EXTERNAL CYBER SERVICES FOR YOUR OPERATIONAL ENVIRONMENTS?



Outsourcing the cyber part makes it possible to work around the lack of internal skills by avoiding recruitment difficulties. Industrial companies can also benefit from the pooling effect to be gained through using these service companies.

Vincent Nicaise, Stormshield industrial partnerships and ecosystems manager

Though perfectly understandable, this use of outsourcing should however encourage industrial companies with confidence in the cybersecurity aspects of their own operational systems to become increasingly vigilant. To avoid an attack to their supply chain, they must ensure that their service providers and suppliers are also well protected.

The SolarWinds case unfortunately showed us that security companies themselves are not exempt from such issues and despite their best efforts can propagate this type of bouncing attack. It all began in 2019 when cyber criminals (Nobelium) gained access to the Orion production system without being detected. This software published by the Texan company SolarWinds, is used in many organisations, companies and industries including several American governmental agencies. In all, they succeeded in infecting 18,000 clients through a malicious update known as Sunburst. Among these, 250 are believed to have permeated worldwide. Discovered in late 2020, this attack has already become a landmark in the history of cybersecurity.

Let's hope that it has brought the subject to the forefront in discussions (and contracts) between partners and suppliers who have no other choice than to collaborate in order to tackle these new threats.

3.2.

Higher budgets to be allocated to industrial cybersecurity

According to the results of our survey, industrial cybersecurity represents less than **10%** of the company's overall budget for **1 respondent in 2**. It accounts for less than **10%** of the IT budget for just over **4 respondents in 10.** Finally, **39%** of respondents feel that this industrial cybersecurity budget will increase over the years to come.

Indeed, the public authorities have shown an interest in modernising industry though without devoting a specific budget to the issue of cybersecurity for OT networks in particular for the time being. The effects of plans such as France Relance or France 2030 therefore only affect the industrial cybersecurity sector indirectly and only concern new investments. These re-industrialisation or digital transformation plans for industry are nevertheless opportunities to enhance cybersecurity.

10%

Half of respondents stated that industrial cybersecurity accounts for less than 10% of the company's overall budget. While 4 out of 10 respondents stated that it accounted for less than 10% of the IT budget.

Machinery is often replaced on a production line by production line basis. This new equipment now includes the notion of cybersecurity although the question arises as to its maintenance and the upgrading of existing systems.

Rodolphe de Beaufort, Assistant General Manager of GIMELEC and Organiser of the CyberOT Club

These investments are still insufficient when considering the true security requirements. It can be difficult to secure budgets for cyber projects which generate no profitability as their role is first and foremost to provide insurance against risks.

Marc Fromager, VP Industrial Automation & End Users, Schneider Electric France

Conclusion

The cybersecurity world has witnessed several cyber attacks generating serious consequences. This news, combined with a series of underlying pointers from our survey, points to an under-estimation of the risks involved. This false sense of security even seems to be affecting companies which have already suffered an attack and have begun taking protective measures.

However, industrial cybersecurity is a vital prerequisite if we hope to undertake the digital transformation of industry without major incidents and build a robust industry 4.0 tomorrow.

The risks posed to industry by the interconnection of networks are (unfortunately) with us for the long haul. It's therefore vital to take account of this and to invest right now in protection for the whole production system, while also recognising that it will continue evolving and so will industrial cybersecurity.

Stormshield Solutions

The basic principles for cyber-securing your industrial IT networks are as follows:
→ Creating an overview
→ Protecting networks through segmentation
→ Authenticating and validating traffic
→ Managing remote access
→ Protecting workstations
→ Adapting security equipment to the operational constraints encountered in industry

To assist you, Stormshield has designed:



→ SNi40 and SNi20, industrial firewall solutions
These firewalls are equipped with reinforced housings to meet the needs of high-stress environments. Easy to mount in electrical cabinets and ideal for all OT network sub-segmentation requirements, they can be installed within the operational system needing to be protected. The SNi40 is specifically designed to protect APIs and PLCs. For its part, the SNi20 is particularly suitable for distributed networks comprised of few PLCs. It's important to note that the SNi40 is the only industrial firewall to have CSPN certification and Standard level qualification from the ANSSI.



→ SNxr1200, for embedded cyber security
This encryption firewall is the only network protection solution built into a tough, mass-produced unit. This secure solution is therefore particularly suitable for tough, high-stress environments - requiring embedded protective equipment.



→ Stormshield Endpoint Security (SES)
The SES solution combines a behavioural analysis engine, a device control engine and a capacity to perform the whitelisting of applications, making any software which is not strictly necessary inactive. And for even more effective protection, proactive security can be maintained even when the workstation is not connected to a management or Internet-based network.

Sources / References

Barometer survey of decision-makers' needs and expectations faced with the deployment of solutions in operational environments - Stormshield/Usine Digitale.

Methodology: self-administered online questionnaire completed between 17th November and 12th December 2021 by 210 decision-makers from the industrial sector.

SOURCES

- Norsk Hydro : une communication exemplaire à l'épreuve des marchés — ZDnet
- Norsk Hydro chiffre à 46 millions d'euros l'impact de la cyberattaque au premier trimestre — Le Figaro
- Frappé par un ransomware, Honda suspend sa production — L'Usine Digitale
- Touché par un ransomware, Honda stoppe sa production — Le monde informatique
- Les leçons de l'attaque « SolarWinds » — La Presse
- Jean-Yves Poichotte (Sanofi) : « Depuis le début de l'année, nous avons bloqué 8 millions de cyberattaques » — Mindhealth
- Visés par une cyberattaque, des sites portuaires européens sont au ralenti — L'Usine Digitale
- Nautisme - le Groupe Bénéteau victime d'une cyberattaque — Actunautique.fr
- Cadres: 8 nouveaux métiers très recherchés dans l'industrie — Capital
- Guide pédagogique de la cybersécurité OT, publication fin avril 2022

The **European cybersecurity choice**

www.stormshield.com

All distribution, reproduction or representation, even in part, of this white paper, for any purposes other than private use, regardless of the medium, is prohibited, and may engage the civil and criminal liability of any person failing to comply with this prohibition.

Copyright © 2022 Stormshield