Industrial Security in 2019: A TÜV Rheinland Perspective

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

Table of Contents

Executive summary

INADEQUATE CYBERSECURITY FOR OT AFFECTS THE ABILITY TO WIN NEW CONTRACTS AND ORDERS

Modern industry, be it manufacturing, telecoms, utilities, transportation or power generation/distribution, is undergoing significant change as new technologies provide better ways to create, build and supply products and services. Adoption of modern technology is challenged by the increase in cybersecurity threats that target the Operational Technology (OT) community.

This is in turn fueled by insert this: Industrial OT operations are also challenged by a requirement across the supply chain to protect confidential manufacturing data. Production systems must maintain an exceptional level of safety, as well as productivity. Lack of an appropriate OT cybersecurity environment can have a direct impact on the ability to win new contracts and orders. Customers will be reluctant to share intellectual property, material and designs with facilities that are vulnerable to cyberattack.

CYBERSECURITY-RELATED POLICIES AND PROCEDURES NEED TO BE TAILORED FOR THE SPECIAL DEMANDS OF OT

As many OT systems have grown over time, an unbounded risk environment has been created as businesses struggle to control their related assets and networks. Without knowing all of the OT assets that need to be secured and then monitoring them on an ongoing basis, it would be extremely difficult to secure an OT estate. You can't manage what you don't know. This challenge is further complicated by connecting business IT systems to the production OT environment and applying traditional information security controls to the often different demands of operational technology systems. Frequently this approach is compounded by using unsuitable IT policies and procedures. Cybersecurity-related policies and procedures need to be tailored for the special demands of OT. Specific policy measures need to be implemented for production sites and facilities. Simply applying current IT information security policies is not sufficient.

GROWING DEMAND FOR BETTER OT CYBERSECURITY

OT cybersecurity incident response plans need to be regularly exercised so that all participants know their roles and responsibilities. This approach will also identify any changes in people, processes or technologies that will impact how a plan is executed. Once an OT cybersecurity incident has been addressed, operations need to return quickly to business as usual.This recovery plan should address the steps that need to be taken to, for example, rebuild OT systems and assets. Failure to plan for such a recovery could significantly impact plant re-start times.

Ultimately, an industrial system that has been compromised by a cyberattack, could potentially cause an environmental disaster, seriously injure people, or cause fatalities. OT cybersecurity needs to be addressed by using a proportionate, risk-based evaluation and the implementation of fully budgeted and resourced OT cybersecurity controls.

This Perspective for 2019 anticipates a growing demand for better OT cybersecurity and urges action today.

Perspective for 2019 – your next steps

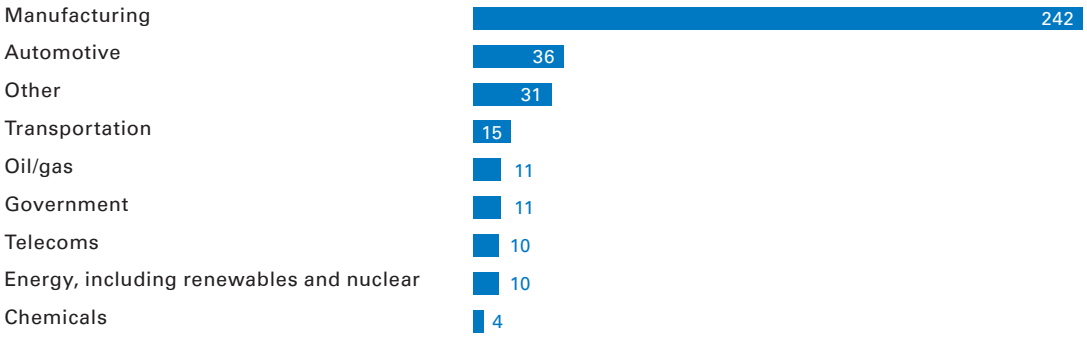
1. With the increase in focused OT-related hacker activity it is now vital that organizations explicitly address their OT cybersecurity risk as a separate, actionable line item.
2. Network monitoring, asset discovery and inventory management should be implemented across all OT systems and a capability developed to respond effectively to any priority event or incident.
3. OT systems workers and production teams need to be fully involved as they form a key layer of cybersecurity defense.
4. IT cybersecurity governance, policies and procedures should be updated to ensure that OT systems are fully incorporated and accounted for.
5. Critical safety systems should be reviewed and steps taken to ensure OT cybersecurity risks are regularly assessed as part of any safety case.

Introduction

An international online survey of 370 industrial organizations was undertaken in spring 2018 by the independent research and analysis company Bloor Research. The objective was to gain insight into how organizations manage challenges to their OT cybersecurity.

Cybersecurity hacks and attacks against electro-mechanical and electronic systems were relatively unheard of prior to the now infamous Stuxnet attack against Iranian nuclear facilities that was publically revealed in 2010 (Zetter, 2014).
Now referred to as OT, this domain, which includes the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices, has been subjected to increased attention from hackers and attackers of all guises.
This 2019 Perspective has been written to cast light on the approaches of those involved with managing and protecting OT estates across different sectors and to uncover prevailing attitudes to OT cybersecurity issues.

FIGURE 1:
What industry sector are you primarily involved with?



This report explores how the threat to OT systems is seen by organizations across different sectors and what effort is being expended to address it. This framework is structured around the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1 - April 16, 2018).
Respondents were self-selecting and there was no specific targeting of types of organizations or sectors as the survey was designed to appeal across the operational technology domain. Most of the respondents were in the manufacturing sector. Some of the survey questions were broad by necessity. For example the term "risk assessment" could also be seen to include a "controls review," so the results are open to interpretation. In this type of survey, it is not possible to collect expansive details from each respondent. As such, this report focuses on the sentiment of each question in order to elicit valid data and highlights key findings.

FIGURE 2:
Which job title most accurately describes your position/role?

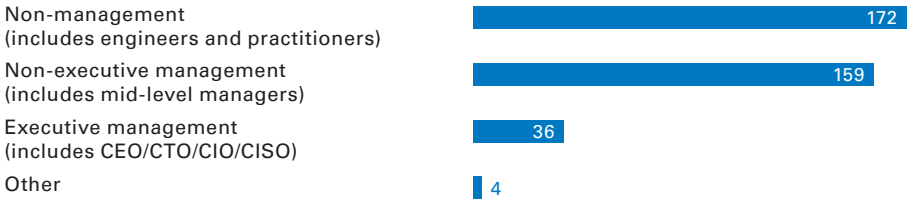
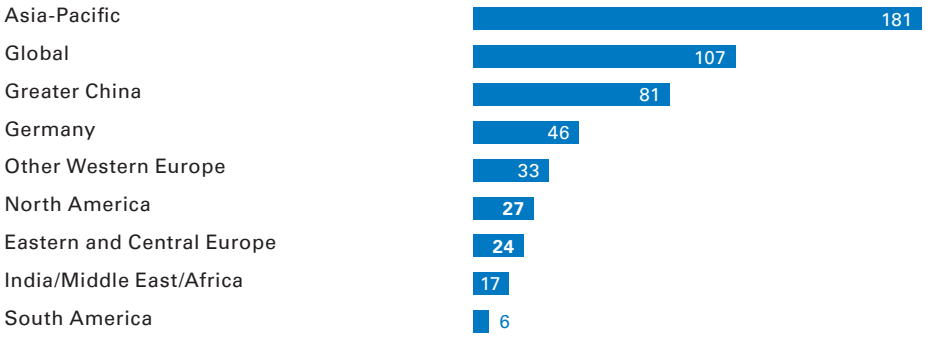


FIGURE 3:
What region(s) are you primarily responsible for? (Multiple Choice)



The importance of OT systems risk assessments

The majority of mature businesses have a good understanding of their risk profile, which can include anything from geopolitical impacts and financial market uncertainty to shortage of raw materials critical to their manufacturing process.

Information security or cybersecurity-related risks have increasingly appeared on the corporate risk register as executives increase their understanding about these issues. Increased knowledge is helped by many well-respected international bodies, such as the World Economic Forum, who have included cybersecurity as a key part of their threat and risk narratives (World Economic Forum, 2018).

2018 Analysis, facts and figures

When discussing risks it is important to understand how IT security differs from OT cybersecurity.

Information technology in corporate organizations is structured to ensure that data confidentiality is maintained, with measures in place to protect its integrity and associated availability.

In many organizations availability may not be a significant business risk; if emails are delayed by 10 minutes many organizations could still function, and there will be no impact on the bottom line. Of course, there are exceptions, but for several companies such latency is acceptable.

Various corporate IT systems have a limited lifespan and, as hardware continues to improve in line with Moore's Law (Intel Corporation, 2018), computer hardware may be swapped out of business every 2-3 years. IT systems should be subject to regular patching and updates as new threats emerge, and vendors rush to patch vulnerable software. In numerous cases, this patch cycle is much easier than in the past as companies understand the need to test and deploy patches in a short time frame, assisted by vendors who release routine patches on a regular, predictable cycle.

The risk profile of operational technology and industrial control systems is often different from mainstream IT systems, and a different attitude must be taken when dealing with them.

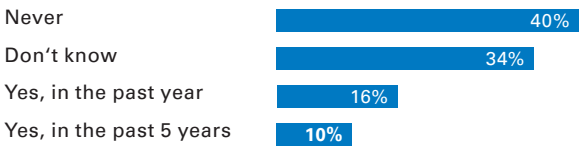
The lifetime of OT systems can often be more than ten times that of a corporate IT system. During this lifetime the control system may be updated infrequently or patched, if at all. This is in stark contrast to the seemingly never-ending patches needed in a corporate IT system.

The rise of internet-connected OT systems presents the traditional control system engineer with a challenge. While a business or OT equipment manufacturer may put pressure on engineers to adopt connected devices (or maybe Industrial IoT devices (Maw, 2018) for cost-saving measures, such as predictive maintenance, this strategy is likely to receive short shrift in a cybersecurity-aware operations room. The thought of connecting devices and systems to the internet by default, without significant security controls, is understandably a step too far for many seasoned OT cybersecurity professionals.

Functional safety, which translates to human safety, should be the number one objective in any operational technology system. Availability is usually key to the business, and the need to ensure that a plant is still operating will normally be a close second to safety requirements. Any system downtime could cost significant money, and in a tight economy this may be the difference between profit and significant losses.

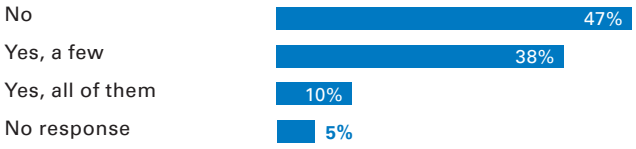
In our question below, 40% of respondents had never conducted an OT risk assessment. Of respondents, 34% didn't know if a risk assessment had been conducted.

FIGURE 4:
Have you ever conducted an OT risk assessment?



Companies that place orders with manufacturers or industrial suppliers are increasingly looking for assurance that OT cybersecurity risks are addressed. Orders may only be placed if there is some assurance that intellectual property, such as CAD drawings, will be protected by the manufacturer. The automotive industry already has its own assessment for this, TISAX (www.enx.com/TISAX).

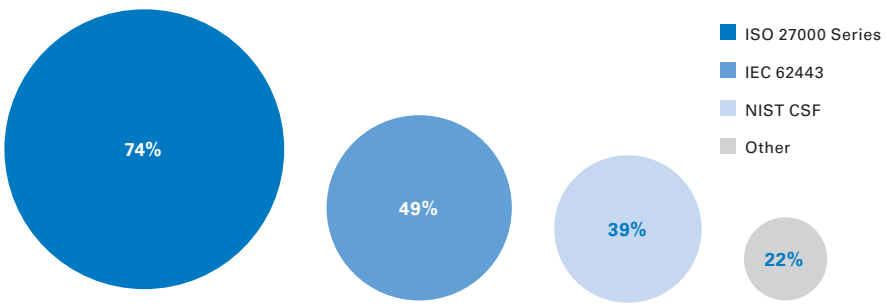
FIGURE 5:
Do your customers explicitly ask you to demonstrate that you have taken steps to secure your operational technology network?



Of respondents, 38% stated that a few or all of their customers asked for evidence that the OT network had been secured. While 47% of respondents stated that they were not asked this question, there is an inevitable demand for supply chain risk management. It is fully expected that an increasing number of manufacturers and industrial suppliers will need to demonstrate that OT cybersecurity risks have been addressed. This requirement will have an interesting effect on budgets and investment in OT cybersecurity measures as demand increases.

A widely used information security management system (ISMS) standard is the ISO/IEC 27000 series. Undoubtedly this is a comprehensive set of standards that provides a bedrock for IT systems information security. With the advent of new OT assessment frameworks its use for addressing such cybersecurity risks will likely diminish. This series was used by 74% of respondents, followed by 49% who use the ANSI/IEC 62443 series (Figure 6).

FIGURE 6:
What frameworks or standards did you use for the [cybersecurity risk] assessment? (multiple selections possible)



This is a set of standards from the American National Standards Institute and the International Electrotechnical Commission that defines procedures to implement cybersecurity across Industrial Automation and Control Systems (IEC). These standards were originally referred to as ANSI/ISA-99 or ISA99 standards.

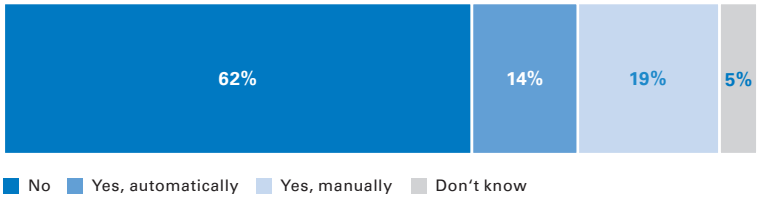
Use of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity was at 39%. The framework was originally developed with the operators of critical infrastructure in mind, but is used by a wide range of organizations. It is designed to help organizations to assess and improve their ability to prevent, detect and respond to security incidents.

Regulations other than these are cited by 22% of respondents, in many cases regulations were very specific to a particular industry sector. Those others used included SAE J3061, JASO TP15002, ISO26262, Pressure Equipment Directive, IATF16949, MIL-STD-882D, NCIIPC, and C2M2. It is interesting to note that not all of these standards are applicable to general OT cybersecurity risk assessments.

Of course, some organizations chose to use one or more standards to conduct this work. This synthesized approach is becoming more common as single standards may not address all perceived risks or issues in a business. This approach is reflected by the fact that both the NIST Framework for Improving Critical Infrastructure Cybersecurity and IEC 62443 pull on other standards to inform their approach.

Of respondents, 62% were unable to detect all of their OT endpoints and only 14% had some form of automatic endpoint detection capability.

FIGURE 7:
Are you able to detect all the endpoints on your operational technology network?



OT cybersecurity risk is rarely called out as a separate risk itself, more often being subsumed into overall IT risk or even considered as part of the production risk because of its effect on lost productivity. Moreover, OT assets can be difficult to track and trace because of the abundance of poorly documented serial networks that have grown over the years to meet production demand.

2019 Perspective – your actions

SENIOR EXECUTIVES

- Address OT cybersecurity risk as a separate, actionable line item. With the increase in focused OT-related hacker activity it is now vital that your organization explicitly deals with this threat.

OT PRACTITIONERS

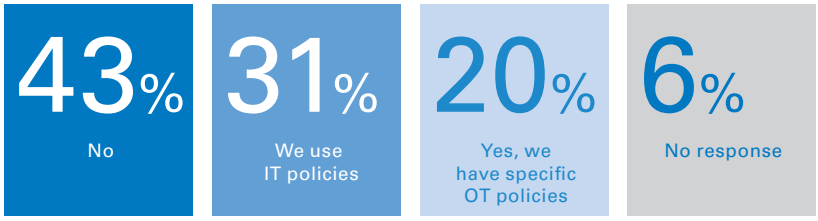
- Understand and limit your risk using suitable frameworks and tools. Consider using products that enable OT assets to be detected automatically, using a non-invasive "light touch" that does not interrupt the OT network or increase traffic that could impact system performance.

Protecting the OT estate from cybersecurity threats

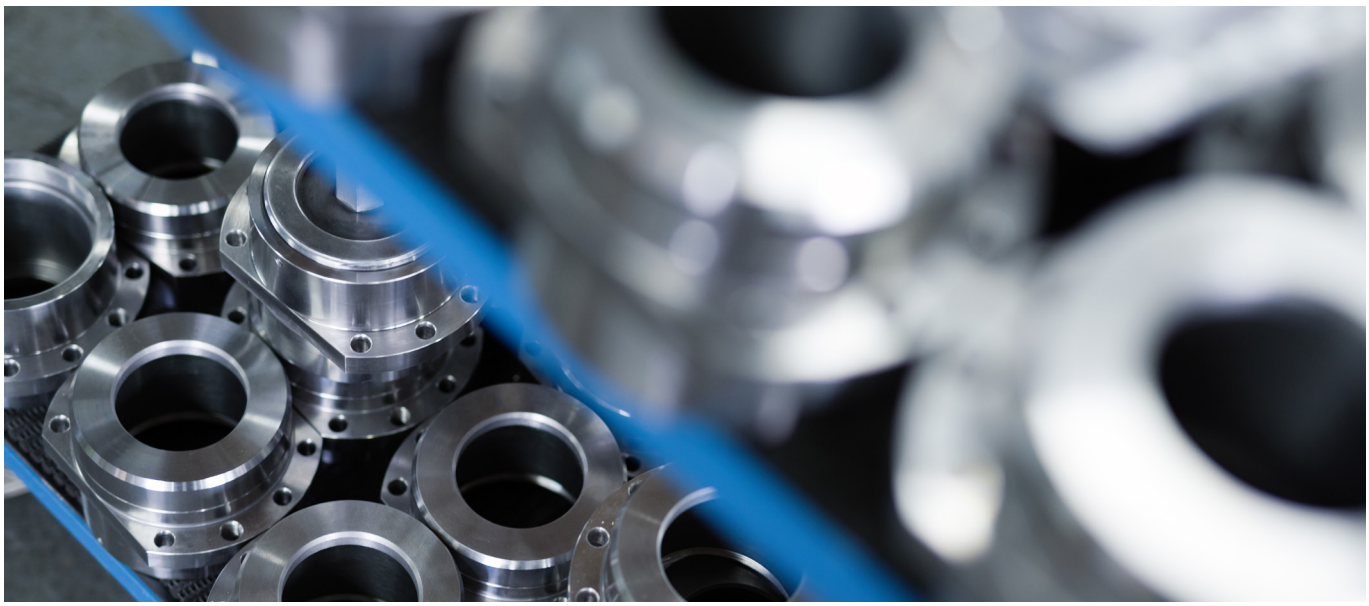
We have seen that understanding and limiting OT systems risk is the first step in addressing the issue. OT systems must be protected using a combination of policies and procedures, technical controls, user education and supporting processes.

2018 Analysis, facts and figures

FIGURE 8:
Have you implemented operational technology-related cybersecurity policies and procedures in your business?

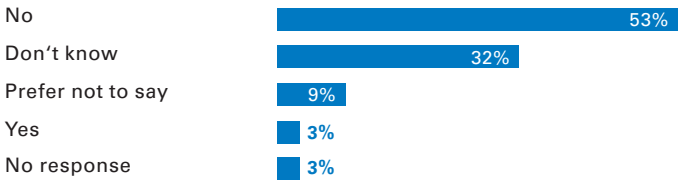


Of respondents, 43% don't have any policies and procedures for their OT systems and 31% rely on the (assumed more general) policies and procedures that have been created by the IT department.



OT systems need to have policies and procedures that have been adapted for that environment, and 20% of respondents have done this. Of course, many IT policies can be applied or repurposed to suit the OT environment, but a conscious process of putting in place these customized policies and procedures is important.

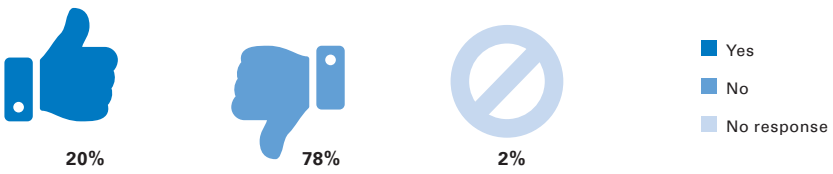
FIGURE 9:
In the past year, have you lost operational technology-related intellectual property (IP) as a result of a data theft?



It is interesting that 53% of respondents were able to assert that they had not lost any OT-related IP in the past year. As expected, a number of respondents would prefer not to say. Although this is an anonymous survey, data losses can be sensitive; and it is understandable if they are not disclosed.

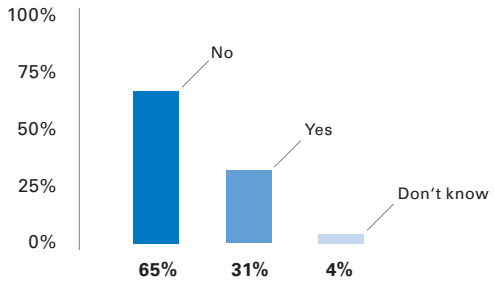
Physical security responsibility often falls under the remit of the facilities management team rather than any cybersecurity related team – IT or OT. In OT plants, the fact that physical security is often managed by a facilities group, not an IT group, is reflected by the fact that most respondents – 78% – had no responsibility for physical security. The 20% of OT cybersecurity teams that do have responsibility for physical security are clearly leading the way in converged security (Figure 10).

FIGURE 10:
Do you have responsibility for the physical security of your plant(s), systems or process networks?



In this survey, 31% of the respondents stated they had OT cybersecurity training and education program in place, whereas 65% of respondents rely on their current information security training.

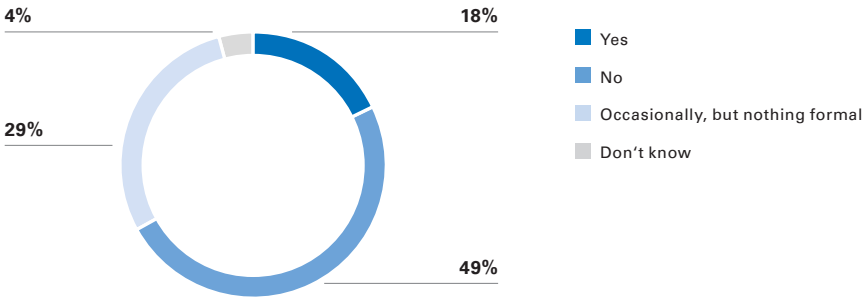
FIGURE 11:
Do you have an OT cybersecurity training and education program in place?



OT threat intelligence sharing is a new idea. Many organizations are only starting to form a picture of their OT risk and associated situational awareness, both key requirements to help build out an internal intelligence model. Once a model is in place, discussions can be had on how this can be shared with sector peers.

Of respondents, 49% don't actively share OT threat-related intelligence with their peers and only 18% do so on a formal basis.

FIGURE 12:
Do you actively share operational technology threat-related intelligence with your peers?



In critical infrastructures this intelligence sharing may be accelerated by government or regulator involvement as key and nationally important systems and processes must be protected as an imperative. It is expected that OT intelligence sharing will grow as its associated value is realized.

2019 Perspective – your actions

SENIOR EXECUTIVES

- Ensure there is a culture of protecting OT-related data in your business. In many cases, the loss of OT data could reveal your organization's confidential business information. This data could include anything from product output to the ratio of ingredients in a production formula – all of interest to competitors. Support should be given to measures to prevent data theft.

- Ensure that there is an OT cybersecurity-related education program across your business. Many organizations have some form of IT cybersecurity education for their staff. An educated workforce can be the eyes and ears of an information security program and will pick up on issues such as phishing emails and misuse of thumb drives or similar storage media. This program should be extended to OT cybersecurity education.

OT PRACTITIONERS

- Don't forget physical security. There is a growing trend towards converged security where we see logical (IT or OT) and physical security coming under a single owner. This makes a lot of sense in many organizations as the physical security of OT assets is critical. Preventing physical access to a production facility or factory can help avoid threat actors from mounting attacks using implants, through to avoiding straightforward thefts. Detecting and taking action on a physical security event or incident may prevent an associated logical attack on OT systems.

- Get everyone involved in your cybersecurity education program. OT cybersecurity training and education need to be adapted to meet the needs of the teams involved from across the business – including the production line staff and executive teams.

- Share and process threat intelligence information to protect your business and the wider industrial community. Threat intelligence sharing has become common in many sectors as business competitors realize there is value in pooling findings and issues to protect the greater whole. No doubt there is an expectation of reciprocity and hope that a competitor may provide some intelligence that could help competing businesses avoid threat and damage. Irrespective of this such intelligence sharing has to beneficial for every OT sector.

Discovering OT cybersecurity events

IT network monitoring solutions have been in place for many years, and most organizations that run business IT systems would have some mechanism in place to monitor and detect cyber threats.

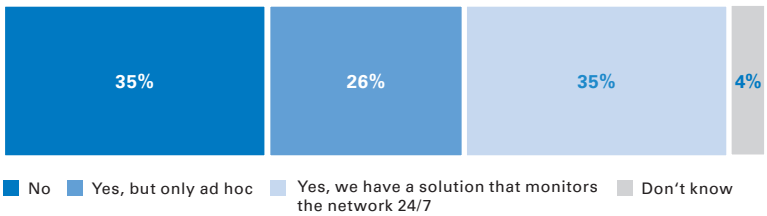
The OT network monitoring industry has rapidly expanded in recent years. A number of vendors have products that detect OT assets and then monitor OT networks to detect cyber threats. A key selling point for many of these solutions is that they are passive and will only listen for network traffic and asset communications. This approach prevents more aggressive and active network scans that could impact the performance and stability of an OT network.

That said, passive scanning has its limitations and careful use of a more active approach may yield much better scan and asset results. The growth of encrypted OT networking protocols will impact passive scanning in the future, so a transition to more active scanning solutions is likely.

2018 Analysis, facts and figures

It was encouraging to see that 35% of respondents have a 24/7 OT network monitoring solution in place, implying that they have visibility across their OT network much in the same way as their IT network.

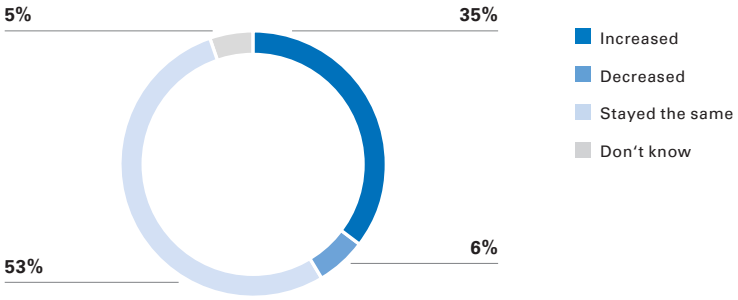
FIGURE 13:
Do you continuously monitor your operational technology network for cybersecurity threats?



Certainly there is increasing interest in attacking such systems – either by "hacktavists," hackers or nation state actors. The media is regularly publishing stories of OT systems` being hacked, and some of the coverage is dramatic and eye catching (Corera, 2017).

Inbound threats to OT systems are therefore likely to increase over time; but this assumes that an organization is in a position to detect the threat in the first place. Most cyber threat analysis processes include a number of steps. Initially, a scope is established that defines what information is needed to improve an understanding of threats. For example, is there a particular make of programmable logic controller (PLC) that is deployed in a plant? – If so, threats to these would be of interest. Data can then be collected from a variety of places, including open-source information on industry and government security forums and product vendor threat databases. This data then needs to be analyzed to draw out further information to affects business risk.

FIGURE 14:
In the past year, has the number of operational technology-related cybersecurity threats to your business...



This cyber threat analysis of OT systems could be a significant change in the way that some organizations manage their process-related risk. It is not surprising that 35% of respondents thought such OT cyber threats were increasing. This trend possibly reflects more awareness and the use of better detection methods. If 53% of respondents believe that the number of threats is remaining the same, that implies that at least they are tracking and recording such threats.

2019 Perspective – your actions

SENIOR EXECUTIVES

- Understand that your business will be subject to OT cybersecurity threats and manage them. Unlike threats to safety, cybersecurity threats are developing, evolving and morphing continuously. In this context, a threat is anything that can attack a vulnerability, such as a software bug, and compromise the confidentiality, integrity or availability of a system.

OT PRACTITIONERS

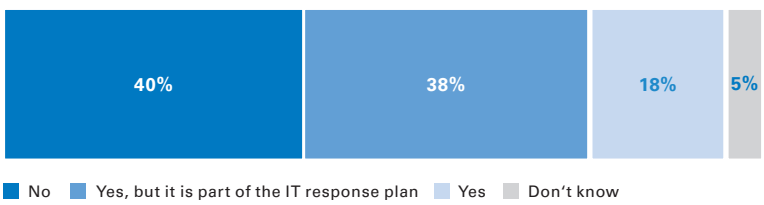
- Build an OT threat intelligence picture. Tying together disparate snippets of data to produce actionable threat intelligence can be complicated, but will help identify areas that the business needs to act upon, which is the final stage in the process. It is only by effectively processing threat data that cost-effective and proportionate action can be taken to protect an OT estate.

Taking action following an OT cybersecurity incident

Once an event or incident has been detected, an appropriate response has to be initiated. A well-rehearsed response plan is critical. If a computer network has not been attacked yet, there is a strong likelihood that it will be attacked in the future. In corporate response plans, OT systems are often forgotten, which can cost dearly after a cyberattack.

2018 Analysis, facts and figures

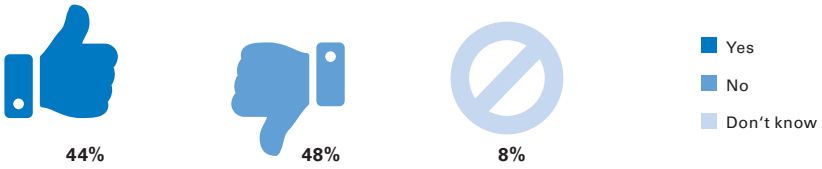
FIGURE 15:
Do you have a specific OT or industrial security incident response procedure in place?



Having a standalone OT-specific response plan is ideal; but if it forms part of the IT response plan, which 38% of respondents stated, that is often good enough as long as any specific OT issues have been identified and remediated. The initial response period is analogous to the medical golden hour where patient outcome can be significantly improved if an effective treatment plan is put in place within an hour of an accident or injury. During the initial OT incident response phase, key team members need to be brought together and an effective strategy quickly established to address the incident based on previous planning and rehearsals.

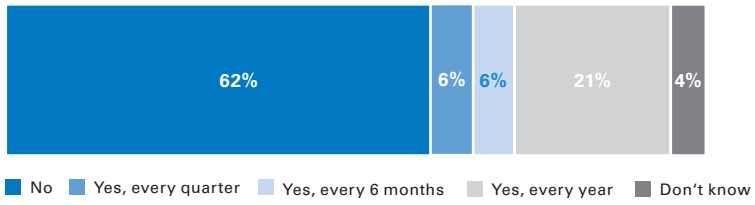
The use of other professionals such as Human Resources, Public Relation and Legal can spread the workload and ensure that non-technical issues are addressed early on, including how staff are managed, how internal/external messaging is initiated, and what the legal framework is for the incident and recovery process. Of respondents, 44% have a plan to use these other professionals in their incidents.

FIGURE 16:
Does your response plan include other professionals such as HR, PR and legal?



How regular an OT response plan needs to be exercised will very much depend on the business in question. There is no single answer other than as often as required. Certainly an annual rehearsal should be the norm; so it is concerning that 62% of respondents don't conduct any form of regular practice of the OT response plan. A lack of practice will lead to a more challenging response when it is required.

FIGURE 17:
Do you conduct regular exercises of your OT response plan?



2019 Perspective – your actions

SENIOR EXECUTIVES

- Ensure that there is an effective and well-rehearsed OT incident response plan in place for your business.

OT PRACTITIONERS

- Rehearse your OT incident response plan on a regular basis. How often will depend on your business and the risks you face; so be informed by the business.

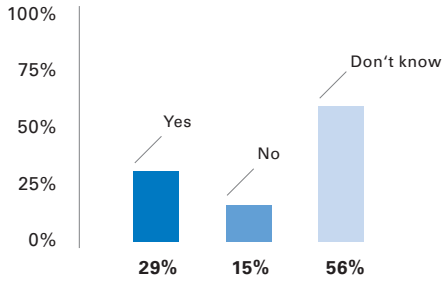
- Build a cross-disciplinary team to respond to OT cybersecurity incidents. The nature of incident/crisis HR, PR and legal advice is often different from that required in day-to-day business: Identify who can provide this specialized input as soon as possible.

Recovering the business following an OT cybersecurity incident

Once an incident has been dealt with and there is no risk of any further disruption or damage a process of recovery needs to be put in place, which would normally include the rebuild and reconfiguration of OT hardware and software so the operation can resume business as usual.

2018 Analysis, facts and figures

FIGURE 18:
Do you have plans in place to recover from an OT-related cybersecurity incident?



It was found that only 29% of respondents had a plan in place to recover from an OT cybersecurity-related incident. The 15% of respondents that had no recovery plan in place would likely face significant challenges to their operation following a major failure.

2019 Perspective – your actions

SENIOR EXECUTIVES

- Ensure there is a formal business recovery plan in place. This is almost as important as having an OT incident response plan.

OT PRACTITIONERS

- Make sure you can support the rebuilding of your OT systems. The recovery plan should consider how OT equipment can be reset, reprogrammed and reconfigured, including the appropriate download/ upload of control software and settings. Without a specific plan in place, OT system configurations would probably not be a part of the OT systems` backup.

Budgets and OT cybersecurity

Budgets play a large part in which processes, procedures and controls can be implemented to secure an OT estate. Operational technology assets and systems may sit in departments separate from the IT department (such as production, facilities or maintenance) so the supporting budgets for OT cybersecurity could be thinly spread, which could mean greater risk to a facility.

If an OT cybersecurity budget is subsumed into the general IT cybersecurity budget again it may not get the budget required to secure OT assets. Insufficient budget is often caused by internal politics or IT teams' not understanding the requirements to digitally secure an OT facility.

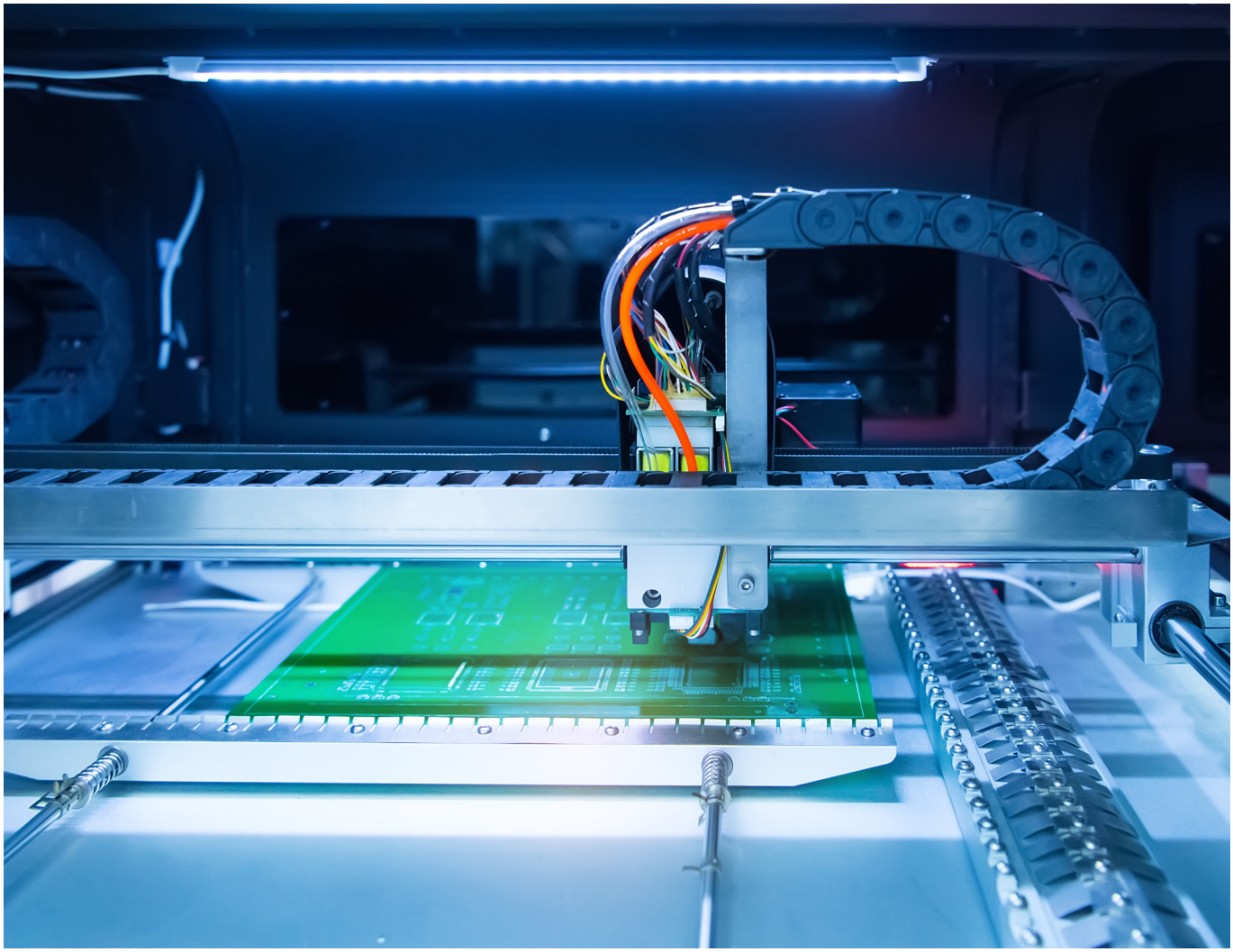
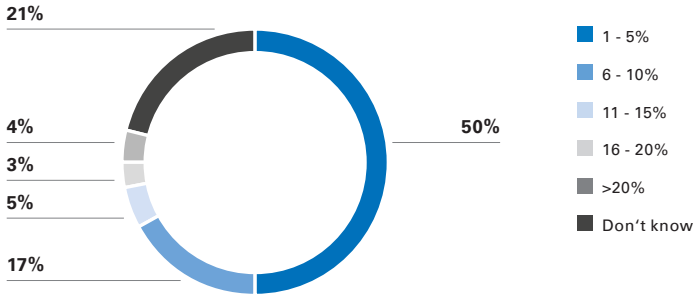
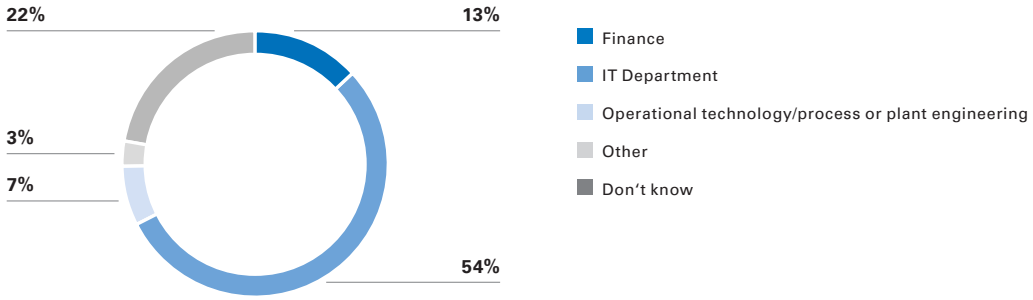


FIGURE 19:
Approximately what percentage of your IT/OT budget do you allocate specifically to OT cybersecurity? (Chose closest value)



Unsurprisingly, 54% of respondents stated that their OT cybersecurity budget sat within the IT department, and 13% in the finance department budget. OT processing and plant engineering only had control of the budget in 7% of the responses. (Figure 20)

FIGURE 20:
Which department has budget for operational technology cybersecurity products and services in your business?



2019 Perspective – your actions

SENIOR EXECUTIVES

- Make sure that OT cybersecurity issues receive an appropriate budget. Few people would suggest that there is an ideal percentage to allocate to OT cybersecurity budgets; but the budget needs to be sufficient to address the relevant OT-related cybersecurity business risk.

OT PRACTITIONERS

- Ensure that OT cybersecurity budgets are under the control of those who really understand the challenges of OT cybersecurity. The trend for IT departments to own OT cybersecurity budgets is likely to increase over the coming years.

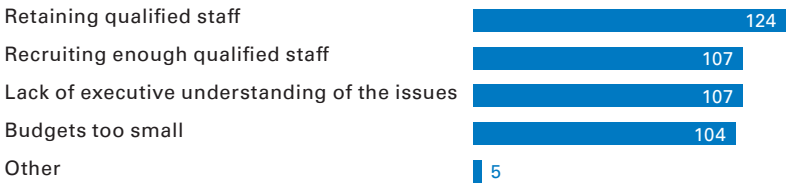
OT cybersecurity challenges

OT cybersecurity is arguably one of the most complex challenges in the OT field as new threats appear with regularity and existing process systems struggle to cope with increasing business demands.

Many OT systems have been in place for decades and only receive just enough care and maintenance to keep them operational day to day. Other OT systems are being introduced that embrace the challenges of Industry 4.0 but may fail to address the associated security challenges of such a hyper-connected initiative (Industrie 4.0, 2018).

2018 Analysis, facts and figures

FIGURE 21:
Within your operational technology cybersecurity strategy, what area provides the most complex challenge? (Multiple Choice)



It is encouraging that 31 % of respondents state that their executive leadership team fully understands the importance of OT cybersecurity measures. It will be interesting to track this measure in the coming years as more stories emerge of hacked OT systems and the awareness of these vulnerabilities improves.

FIGURE 22:
Does your executive leadership team fully understand the importance of OT-related cybersecurity measures?

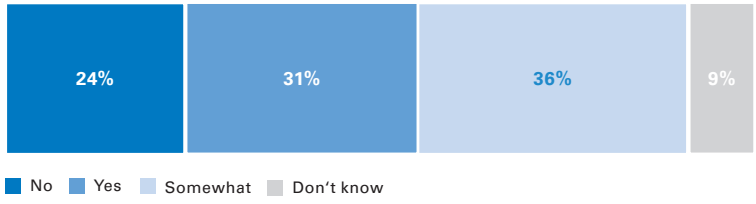
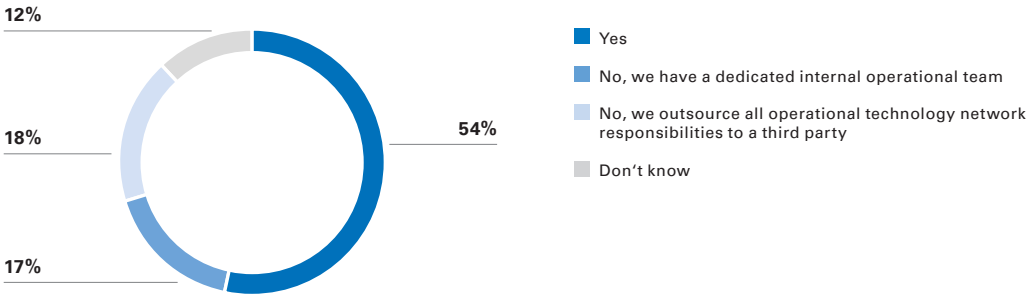
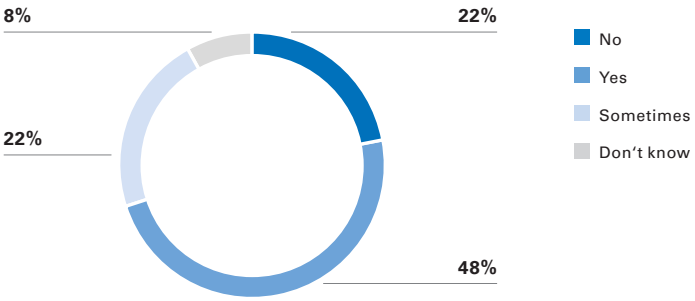


FIGURE 23:
Does your IT team have responsibility for managing the OT network?



Of respondents, 54% stated that the IT team have responsibility for managing the OT network and 18% are able to outsource this to a third party. This response probably reflects a move to managed security services by some organizations. 17% of respondents have a dedicated operational technology team, which is understandable for more complex environments and estates where such outsourcing would be difficult.

FIGURE 24:
Do you assess or review cybersecurity issues when conducting safety-related assessments?



The worlds of functional safety and cybersecurity are now inextricably linked in modern plant and process control systems.

Functional safety is the defense against random and systematic technical failure to protect life and environment. Cybersecurity, on the other hand, is the defense against negligent and willful actions to protect devices and facilities.

Even if a plant has been rigorously designed for functional safety, it can still be compromised by cyberattack. The control systems may be well designed and implemented; but if the HMI (Human Machine Interface) industrial PC is not "locked" using basic security measures systems they could be tampered with.

Of respondents, 48% assess or review cybersecurity issues when conducting safety-related assessments, but 22% don't. With an increasing number of international safety regulations now asking for cybersecurity risks to be evaluated when conducting safety assessments, the number of those not conducting cybersecurity risk assessments as part of their safety case will inevitably decrease.

2019 Perspective – your actions

SENIOR EXECUTIVES

- Build a good OT cybersecurity team to support your business. Keeping qualified staff who understand process technologies and cybersecurity is essential to defend your business against cyberattack.

OT PRACTITIONERS

- Continue to educate your business leadership on the importance of addressing OT cybersecurity issues. Lack of executive understanding is regularly cited by cybersecurity practitioners as a major frustration. This refrain is often reciprocated as business leaders complain about the lack of understanding of the business demonstrated by the same practitioners.

About Bloor

Bloor is an independent research and analyst house focused on the idea that Evolution is Essential to business success and ultimately survival. For nearly 30 years we have enabled businesses to understand the potential offered by technology and choose the optimal solutions for their needs.

Bloor was founded in 1989 around one principle: "To enable organizations to choose the optimal technology solutions for their success," we provide actionable strategic insight through our innovative independent technology research, advisory and consulting services. We assist companies throughout their transformation journeys to stay relevant, bringing fresh thinking to complex business situations and turning challenges into new opportunities for real growth and profitability.

In the age of mutable business, Evolution is Essential to your success. Bloor brings fresh technological thinking to help you navigate complex business situations, converting challenges into new opportunities for real growth, profitability, and impact. We'll show you the future and help you deliver it.

www.bloorresearch.com

About TÜV Rheinland

Business Stream Digital Transformation & Cybersecurity
For more than 20 years, our mission at TUV Rheinland has been to help our clients with safe and secure use of technology by combining our digital transformation and cybersecurity expertise with unparalleled industry know-how.

Our services portfolio spans innovative solutions for digitalization with smart data, critical infrastructure and connected solutions delivered by highly experienced consultants. Our approach to cybersecurity solutions offers a unique fusion of security, privacy and safety in an increasingly more vulnerable world of interconnected cyber-physical systems and devices, with pragmatic solutions for mastering enterprise risk, analytics-based threat detection, automated and manual cybersecurity testing, industrial security, IoT data privacy, and secure cloud infrastructures.

With a team of nearly 1,000 consultants around the globe, we deliver advisory, consulting, testing and managed services to our clients across all industry segments as well as public safety authorities, government organizations and public institutions. TÜV Rheinland runs a worldwide network of more than 100 advanced testing laboratories offering our clients a one-stop-shop for all their testing needs from product safety to cybersecurity and privacy protection.

www.tuv.com/informationsecurity

References

Corera, G. (2017, December 30th). If 2017 could be described as 'cyber-geddon,' what will 2018 bring? Retrieved from BBC: https://www.bbc.com/news/technology-42338716

Industrie 4.0. (2018, August 14th). What is Industrie 4.0? Retrieved from Plattform-i40: https://www.plattform-i40.de/I40/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html

Intel Corporation. (2018, August 28th). 50 Years of Moore's Law. Retrieved from intel.com: https://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html

Maw, I. (2018, February 15). How to Use the Industrial Internet of Things (IIoT) in Your Factory. Retrieved from Engineering.com: https://www.engineering.com/AdvancedManufacturing/ArticleID/16506/How-to-Use-the-Industrial-Internet-of-Things-IIoT-in-Your-Factory.aspx

National Institute of Standards and Technology. (2018, April 16th). NIST. Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

World Economic Forum. (2018, January 24th). To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity. Retrieved from World Economic Forum: https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/

Zetter, K. (2014, November 3rd). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Retrieved from Wired: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Cologne
Germany
otsecurity@tuv.com

www.tuv.com/en/ot

TÜVRheinland®
Precisely Right.