SIEMENS

IMPORTANCE OF A SOLID DEFINITION OF

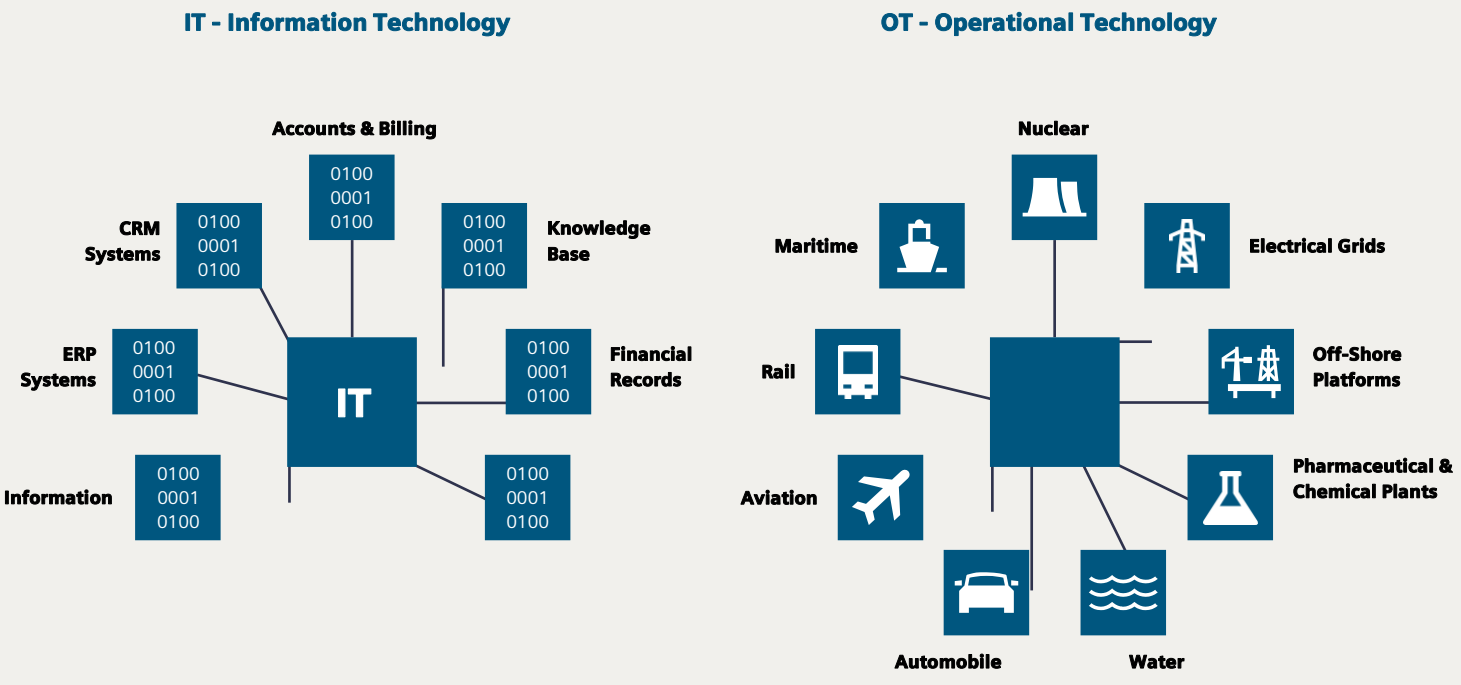
Operational Technology in cybersecurity legislation

Uniform rules of play and a level playing field to achieve a cybersecure business sector via standards, monitoring, enforcement and collaboration.

Operational Technology in cybersecurity legislation

In this mini-paper, we address the importance of OT cybersecurity for you as an owner of OT systems (alongside your IT systems) and/or as a regulatory institution.

In this paper, the term 'Operational Technology' is defined as: equipment and software intended for control of bridges, the rail network, our drinking water supply, electricity and gas supplies, controls within factories, etc.



Charter of Trust

Digitization has changed practically every aspect of our lives. Nowadays, billions of devices are connected to the Internet of Things. This creates wonderful opportunities, although it also involves major risks. In order to create a safer digital world, Siemens aims to pool the strengths of a wide variety of companies by means of the Charter of Trust. This unique collaboration between leading businesses has resulted in vital improvements in the field of cybersecurity. The goals for the future are ambitious.

The Charter of Trust (www.charteroftrust.com) focuses on three objectives:

- Protecting data belonging to people and businesses
- Preventing people, businesses and infrastructure from suffering damage or loss
- Establishing reliable digital foundations upon which widespread trust in our interconnected digital world can develop and flourish.

Strengthening the chain

Cyber risks in the supply chain are increasing. The digitization of industry (accelerated by the Covid-19 pandemic) has resulted in greater dependence on an increasing number of external partners, suppliers, service providers, contractors etc. and a single security incident affecting a single supplier can therefore substantially disrupt an entire fully integrated supply chain process.

For this reason, we must explore ways to better identify shared vulnerabilities or dependencies and address gaps in policy as this will boost security and resilience within the supply chain. This approach can help establish a joint certification mechanism based on international standards and certification regulations in addition to broader holistic principles concerning cybersecurity, as well as helping to build upon cybersecurity recommendations championed by the industry. For example, the basic security requirements of the Charter of Trust in the digital supply chain.

NIS 2 Directive: chance of a prominent position for OT

The Network and Information Systems (Security) Act *(Wet beveiliging netwerk- en informatiesystemen* or Wbni) came into force on 9 November 2018. The objective of the Wbni - which is derived from the European Union's NIS Directive- is to boost the Netherlands' digital resilience, with a particular focus on essential suppliers, the government and digital service providers. The act is designed to limit the impact of cyber incidents among these groups to the greatest extent possible in order to prevent social disruption. Despite this legislation, the number of cyber risks continues to grow.

Due to the digital transformation of society, which was accelerated by the Covid-19 crisis and now also by the war in Ukraine, the number of threats is increasing and we are facing new challenges that require original and innovative responses. In order to tackle these challenges and to close the gap between cybersecurity risk perceptions versus actual cyber risks, the European Commission has adopted a proposal to establish an amended directive governing the security of network and information systems (the NIS-2 Directive).

Importance of a prominent position for OT in legislation

Operational Technology (OT) is an aspect of cybersecurity legislation that has received insufficient attention as the focus of cybersecurity legislation has traditionally been on the IT landscape. This is a growing problem given the ever-increasing number of connected devices in the OT environment within the business and industrial sectors. OT-side cybersecurity risks affecting Essential Service Providers (ESPs) can be much more drastic and far-reaching for businesses and society than cybersecurity risks on the IT side. For example, if the electricity supply is shut off for multiple days, the drinking water supply is contaminated or the train network is brought to a halt, then this can have an enormous impact on society.

In addition to IT cybersecurity, Siemens is calling on the government to give OT cybersecurity a much more prominent and explicit position when implementing the NIS 2 Directive in the Netherlands. The following is a number of reasons derived from professional practice of why this is an important issue to our clients.

Increasing cyberthreat level is forcing more and more businesses to take measures.

DI, 12/04/2022 - 07:57 • https://www.winmagpro.nl/nieuws • SECURITY NEWS • *By: Editorial team of WINMAG Pro*

45 per cent of surveyed businesses have had issues with cybercrime in 2022.

Sharp increase in the number of businesses (+55 per cent) targeted compared to last year.

The number of Dutch businesses that have undergone a cyberattack in recent months has increased by over half last year's rate to 45 per cent. In April 2021, just under three in ten businesses reported being affected by cybercrime, while now the figure is almost half. This is the result of a study by ABN AMRO that surveyed 233 business clients who are partly or fully responsible for cybersecurity within their firm. As a result of extensive digitization, which was greatly accelerated by the Covid crisis, the number of potential access points for cybercriminals is increasing rapidly and they are also becoming increasingly sophisticated. Although the identified increase in cyber incidents is a separate issue to the war in Ukraine, this development does call for greater vigilance. For example, the National Cyber Security Centre (NCSC) estimates the likelihood of targeted attacks on Dutch businesses to be low, but warns about collateral damage. After all, in the past, politically motivated cyber attacks on Ukrainian targets have already resulted in major losses for businesses elsewhere in Europe.

Source: https://www.winmagpro.nl/toegenomen-cyberdreiging-dwingt-steeds-meer-bedrijven-tot-maatregelen

Interconnectedness of IT and OT

To gain greater insight into this issue, businesses are increasingly connecting IT and OT systems. This is not only useful for organizations, it is also convenient for hackers as it makes it easier to switch back and forth between the two environments.

Use of outdated and vulnerable software

The characteristics of OT are different to those of IT (see diagram below). OT investments are often major investments for the long term and in general, the availability of these systems must be very high. As a result, many manufacturers and other companies work with older or outdated OT that desperately requires an upgrade. However, closing down production to implement updates is extremely costly, so the software tends to contain a higher number of vulnerabilities and therefore poses an increased cybersecurity risk.

IT - Information Technology

Characteristics	
Life time	3-5 Years
Availability req.	Medium, Delays accepted
Real time req.	Delays accepted
Physical Security	High (for critical IT)
Application of patches	Regular/scheduled
Anti-virus	Common/widely used
Security testing/audits	Scheduled and mandated

OT - Operational Technology

Characteristics	
Life time	Up to 20 Years
Availability req.	Very High
Real time req.	Critical
Physical Security	Very much varying
Application of patches	Slow/none
Anti-virus	Uncommon
Security testing/audits	Occasional

Perceived risk lags behind actual risk

The research shows that although the level of cyberthreats has increased, perception of the risk level has not. "In 2021, three out of ten companies said they perceived cybercrime to be a major risk, and this number has not risen significantly this year. This means that the digital resilience of businesses will only have increased to a limited extent. The extent to which businesses take measures against cyberattacks is closely correlated with their risk perception. We have observed that risk perception is highest among businesses who have been affected by cyberattacks or phishing scams in the past," explains Julia Krauwer, Sector Banker for Technology, Media & Telecom at ABN AMRO. "Although the increase in risk perception is only modest, we have observed that the willingness of businesses to arm themselves against cybercrime is increasing. This is a crucial factor, as business owners have a lot to lose. We found that they are most concerned about losing access to their systems, which confirms how dependent many firms are on digital solutions. By taking measures such as installing antivirus software and a firewall and educating staff to increase their awareness of risks, they can better protect themselves against the substantial operational risks that cybercrime poses."

Source: https://www.winmagpro.nl/toegenomen-cyberdreiging-dwingt-steeds-meer-bedrijven-tot-maatregelen

Few security requirements in place for hardware and software
When purchasing new OT -which are often plug-and-play solutions- businesses frequently pay insufficient attention to cybersecurity. The level of security often leaves a lot to be desired. A more solid approach would be to establish specific cybersecurity standards with which all new OT must comply.

Insufficient monitoring
Within the OT environment, businesses often conduct little to no monitoring of unusual behavior by employees or hardware, as a result of which hackers can move freely between the OT environment and the IT environment, or even take all of the systems hostage.

EU ambition: become world leader in cybersecurity
The EU's ambition is to become world leader in the field of cybersecurity. This means that cybersecurity should be a default aspect for products and suppliers of IT, OT and IoT products as well as for businesses that use these products. This goes further than simply selecting the right technology: it's also about setting up processes and influencing staff behavior. Currently, companies -including ESPs- have a certain degree of freedom to choose the required level of cybersecurity. However, within the business sector -and certainly for the ESPs- cybersecurity must no longer be an optional extra and it must no longer be ignored or avoided due to the cost.

Digital resilience 'below par' in the Netherlands while cyberthreat level increases

13 April 2022, 11.13 a.m.

The Dutch business sector has to play catch-up in the field of cybersecurity. Most organizations do not have a digital resilience strategy and security budgets are often insufficient. The Netherlands is also lagging behind when it comes to security awareness training. These were the conclusions drawn by an international study by cybersecurity firm Mimecast.

Source: https://www.engineersonline.nl/nieuws/id35423-digitale-weerbaarheid-nl-bedrijven-ondermaats-terwijl-cyberdreiging-toeneemt.html

It is vital that the government ensures a level playing field when it comes to cybersecurity. Stakeholders must be given equal market access and conditions of competition. Uniform rules of play and a level playing field will help achieve a cybersecure business sector via standards, monitoring and enforcement. Currently, a simple set of standards and guidelines is lacking and the monitoring of cybersecurity is still in development.

The most effective approach for building trust is to adopt a consensus-based international strategy that gets all parties within the standardization process involved and preferably gives market parties a leading position in the process. The development of standards in line with systems such as ISO and IEC will greatly facilitate efficient collaboration with regard to international standards. Subsequently, the government should actively encourage businesses in all sectors to certify their business processes based on international standards such as ISO 27001 and IEC 62443 and ensure that their legislation refers to the same series of coordinated international standards.

In conclusion, if the ambition is to become a world leader in cybersecurity, then it will be vital to include cybersecurity in national education curricula and permanent professional development. Employees at all levels of the public and private sectors must boost their cyber awareness in both their work lives and personal lives. For this reason, Siemens is calling on the business sector and the government to establish pansectoral collaborations to strive towards a cybersecure culture within every business. The recommendations from the Charter of Trust can facilitate this process.

The war for talent is a serious problem

Another major problem identified by the researchers is the 'war for talent'. According to most of the businesses surveyed, it is extremely difficult to find sufficiently qualified security professionals. More than half of the businesses reported having had projects fail due to the lack of sufficiently skilled staff

and they also have great difficulty retaining security professionals. Many security specialists within companies are under great pressure and are often allocated responsibilities that they are not ready for. As a result, they are put under extreme pressure, which often prompts them to consider seeking alternative employment.

Source: https://www.techzine.nl/nieuws/security/484805/cyberaanvallen-nemen-toe-en-securitytalent-wordt-schaarser/

Cybersecurity by design

In order to increase security levels, cybersecurity should be 'built into' products and constantly taken into consideration. As early as the design stage, cybersecurity must be constantly taken into consideration in order to achieve the highest appropriate level of security and data protection. This will help ensure that cybersecurity is preconfigured into the design of products, functionalities, processes, technologies, operations, architectures and business models. The principle must cover more than just a specific product or technology. It is vital to integrate the dimensions of 'people' and 'process'. This can vary from offering basic security training for a company's employees to complying with secure development principles and ensuring solid cyber-risk management. This will help to prevent potential vulnerabilities, cyber risks and the associated costs.

The operation model for cybersecurity:

Risk mitigation across these three dimensions

- → Awareness
- → Skills & Qualification
- → Competent resources
- → Follow the procedures

- → Governance
- → Security framework and policies
- → Operational processes
- → Compliance to standards
- → Audits

Within this scope, the Cyber Resilience Act, which is expected in the third quarter of 2022, is highly relevant. The goal of this act is to protect consumers and businesses against unsafe products. This objective will be achieved by implementing cybersecurity rules for manufacturers and sellers of tangible and intangible digital products as well as providers of associated services. IT, OT and IoT products and associated services will have to be defined and fall within the scope of the law. Only then will we be able to prevent unsafe IT and OT products from entering the EU market and establish uniform standards with which such products must comply.
This will result in a more level playing field and a cybersecure environment.

More information

Would you like more information about cybersecurity in relation to Operational Technology or do you have any questions about this issue? If so, then get in touch with your contact person within Siemens or:

Ivo van Nimwegen, Cybersecurity Manager
ivo.van.nimwegen@siemens.com
06 - 22 30 61 62

→ Ton Mes, Information Security Professional
ton.mes@siemens.com
06 - 22 25 04 78

→ Angelique Kuut, Government Affairs
angelique.kuut@siemens.com
06 - 31 64 13 60

→ Ruud Welschen, OT security services professional
ruud.welschen@siemens.com
06 - 55 84 49 11

Annex:

Global

A global survey of >1,200 leading cybersecurity professionals has revealed an increase in identified attacks and a growing number of breaches. 65% of organizations report being targeted by a greater number of attacks and 49% says that in the past two years, they have suffered a data leak (compared to 39% one year ago).

Ransomware attacks are increasing and more and more organizations are being forced to pay. Of the respondents who fell victim to a successful ransomware attack, 66% paid the ransom and just 33% restored their systems from a backup. There is a suggestion of overconfidence in a significant proportion of the respondents given that just 42% -particularly those who have not yet fallen victim to a cyberattack- think that their organization will pay the attackers.

On average, the annual cost of cybercrime-related shutdowns within the group of respondents is $33.6 million

and 59% of the cybersecurity teams say that they have had to devote substantial time and resources to recovery efforts. Nearly a third of their time is spent on responding to emergencies rather than preparing themselves for attacks within the supply chain, ransomware attacks and other sophisticated attacks.

Source: https://www.splunk.com/en_us/blog/security/state-of-security-research-details-essential-strategies-for-the-year-ahead.html

Less attention paid to cybersecurity in the Netherlands

In many areas, the Netherlands is lagging behind. Only 30% of Dutch organizations have made progress since last year with regard to coordinating their cyber strategy with their business strategy. In addition, less progress has been made in getting CEOs involved in the issue of cybersecurity (68% in NL compared to 79% worldwide). Furthermore, the amount of time spent on cybersecurity during board meetings increased at a higher rate worldwide: 39% compared to 30% in the Netherlands.

Businesses also have limited insight into cybersecurity measures implemented by their collaboration partners. Worldwide, less than half (40%) of the respondents reported that they keep track of possible data breaches affecting third parties by means of official reviews, while in the Netherlands, the figure is just 35%.

The percentage of companies that manage risks relating to the software supply chain (the provision of software) is even lower, with 34% of worldwide organizations and just 20% of Dutch businesses keeping track of these risks via official reviews.

Source: PWC, Cyber Digital Trust Insights NL 2022: https://www.pwc.nl/nl/actueel-en-publicaties/diensten-en-sectoren/technologie/bestuurders-niet-betrokken-cybersecurity.html