

CYSSME CyberSecurity for Micro, Small and Medium Organisations

Empowering SMEs :
Cybersecurity Strategies for a Secure Digital Future

Ulrich Seldeslachts,
Leuven (BE), July 3, 2024



© CYSSME - LSEC, 2024, Private & Confidential - Closed User Group Distribution - Do Not Distribute -
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101128101





CYSSME offers cybersecurity services for European micro, small and medium-sized businesses up to 250 employees or 50m euros in consolidated turnover.

cysme.eu



CYBERSECURITY WITH MEs AND SMEs



57%

of small and medium enterprises experienced a cybersecurity breach



26%

of medium sized companies have experienced cyber crime in the last 12 months



> \$500K

Duvel-hackers demanded more than half a million dollar: 'We operate from Lithuania and Russia'

Sources <https://guardz.com/go/survey/> - 2023 - Cyber security breaches survey 2023 - De Morgen, 2024

CYBERSECURITY WITH MEs AND SMEs

- Micro businesses are most likely to **solely use internal staff** to undertake audits (44% of the micro businesses undergoing any type of audit)
- Small businesses have the greatest tendency (44%) to **only use external contractors**
- One of the common behaviours among organisations that developed a **formal strategy** was **to have cyber security break away from another department like IT, facilities**
- **“Spending is usually reactive.** If there is a problem, then it is fixed. We don’t have budget set to go towards cyber security. It’s hard to gauge, as you do not know the extent of data attacks and its cost”. – Purchasing and IT Manager, small business



Cyber security breaches survey 2023

© CYSSME – LSEC, 2024, Private & Confidential – Closed User Group Distribution – Do Not Distribute –
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101128101



CYBERSECURITY OFFERING

CyberSecurity for European Micro and Small, Medium sized Enterprises by European CyberSecurity solutions and expertise SME providers

CYBERSECURITY MATURITY IMPROVEMENT

1

NETWORK AND END POINT SECURITY
immediately protect network and computers.

2

THIRD PARTY RISK
your and your supplier's vulnerabilities visibility

3

COMPLIANCE MANAGEMENT
dashboard and underlying tools
Be prepared for NIS2.

4

INDUSTRIAL
detecting, monitoring and controlling operational appliances

PARTNERS

 <p>AXS GUARD INTERNET SECURITY SOLUTIONS</p>	 <p>IT & SECURITY BA WE KNOW HOW!</p>	 <p>Ceeyu</p>	 <p>CROSS-BORDER CBCOMMERCE.EU</p>
 <p>CYBER TRUST AUSTRIA</p>	 <p>EXALENS®</p>	 <p>L3CE</p>	 <p>LSEC LEADERS IN SECURITY</p>
 <p>Lupasafe</p>	 <p>Nocode-x</p>	 <p>TOREON Business driven cyber consulting</p>	 <p>unizo</p>

CYBERSECURITY IS A PROCESS

Supported by people and technologies, you can improve your situation. We can help you identify where, how and define priorities. CYSSME can support in making the right choices, setting the priorities and getting actionable on what needs to be done.

CYBERSECURITY MATURITY IMPROVEMENT

1

INTERACT

It's not all about tech. We love to hear your story

2

MATURE

CYSSME is interested in helping you grow your business

3

END GOALS

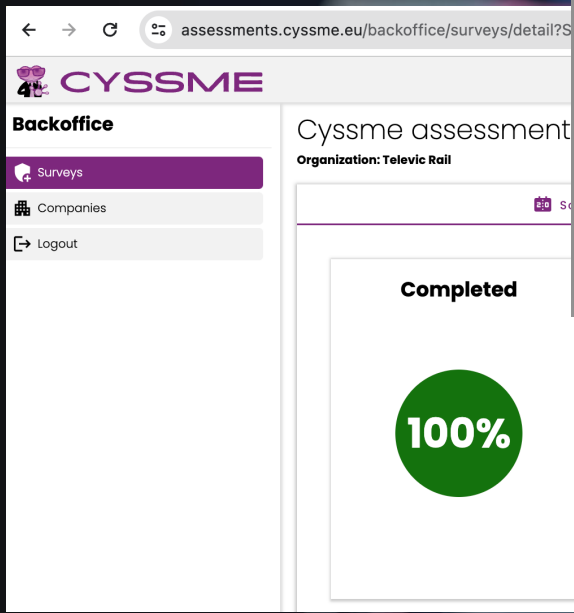
Cybersecure your team, your operations, or supply chain

4

COMPLY

NIS/2, CRA, ISO, GDPR, ... our experts lead you the way.

MEASURING YOUR LEVEL OF MATURITY



Choose your survey



Cyssme assessment

Short & efficient questionnaire for a quick assessment of your security posture based on the most essential security requirements. The result will give you a good orientation where your security is at the moment and which are your most important improvement areas.



Cyberfundamentals

Comprehensive & advanced questionnaire for an in depth assessment of your security posture. The result will give you a thorough understanding of where your security is at the moment.

score



TARGET AUDIENCES



RETAIL

- Medium
- Small
- Micro




HIGH TECH

- Medium
- Small
- Micro



INDUSTRY

- Medium
- Small
- Micro



OTHER

- Medium
- Small
- Micro

CYSSME

Use Cases

© CYSSME – ISEC, 2024, Private & Confidential – Closed User Group Distribution – Do Not Distribute –
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101128101



INDUSTRY

COMPANY PROFILE

- Industry - manufacturing
- ICT - engineering

KEY FACTS

- 130 FTE's
- 30+ years in operations
- Part of larger industrial group
- No Cybersecurity team, only IT manager

KEY REQUIREMENTS

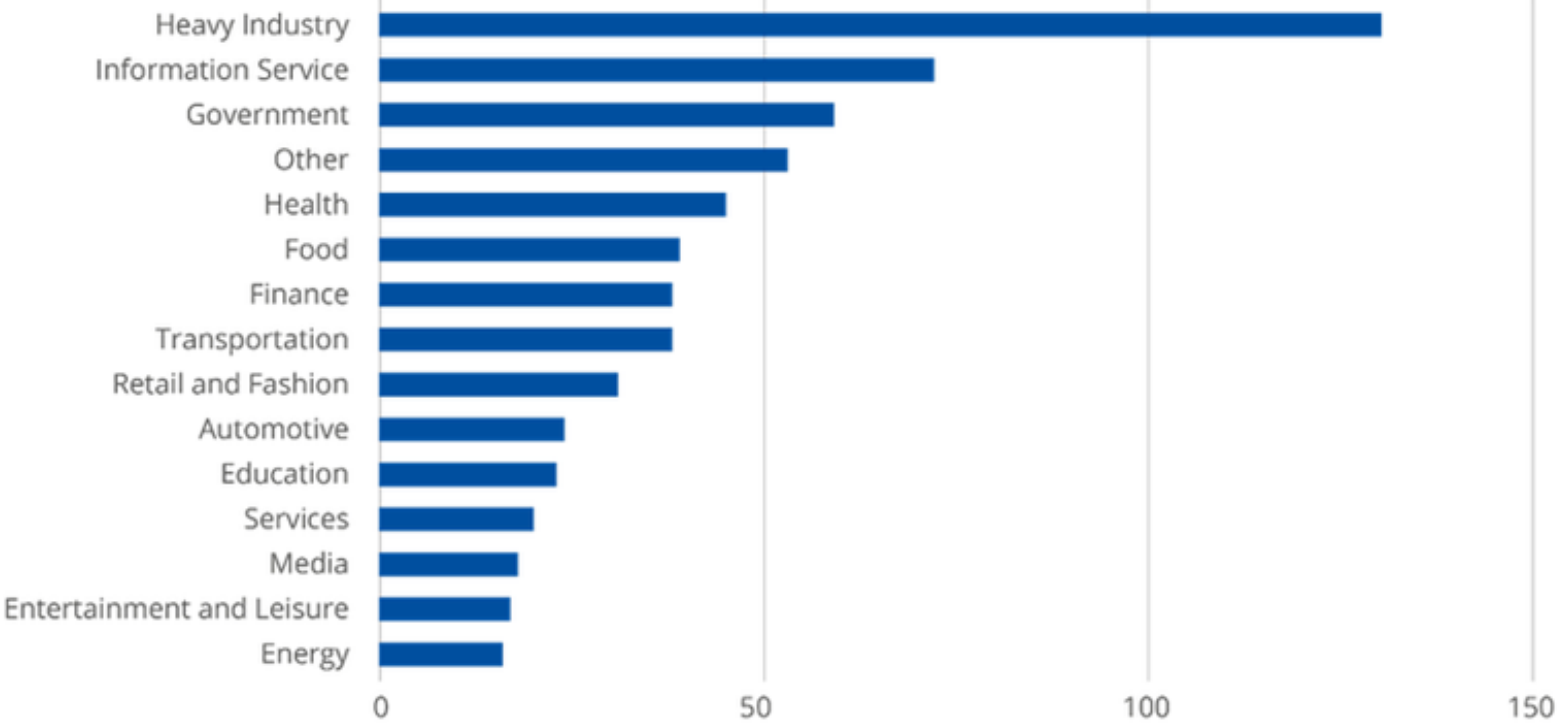
- Making sure they can be Cybersecurity representative towards their customers
- Improving overall on corporate level with Cybersecurity

PROPOSITION

- Improving Cybersecurity-maturity
- Assessing key challenges
- Improving software and technology developments
- Ensuring key challenges are met that would be required from customers – CS standards references (NIST, ISO, ...)
- CISO ad interim and support in selection of CISO



Cyber Incidents 2023 : Manufacturing continues to be target



CyberSecurity Problematiek : Manufacturing continues to be target



LockBit Ransom



Conti Ransom

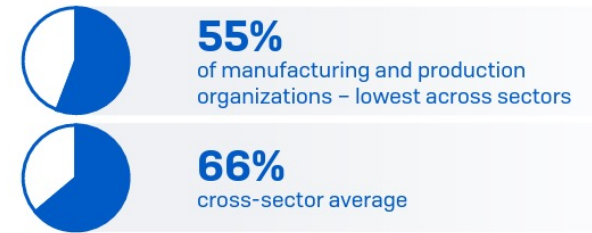


Hacktivists

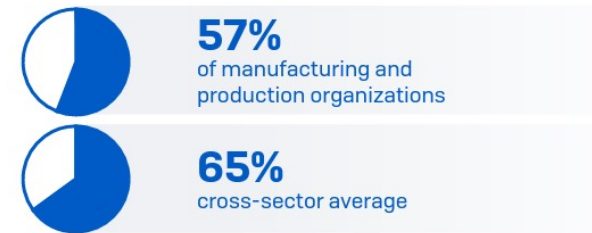


Cyberwarfare

Hit by ransomware



Data encrypted in the attack



Increase in volume, complexity, and impact of attacks over the last year

	INCREASE IN VOLUME OF CYBER ATTACKS	INCREASE IN COMPLEXITY OF CYBER ATTACKS	INCREASE IN THE IMPACT OF CYBER ATTACKS
Manufacturing and production	61%	66%	51%
Cross-sector average	57%	59%	53%

x-IoT Security (inc IIoT) ...in 2023



Legacy attacks: Attacks on xIoT assets for the sake of the xIoT assets & opportunistic attacks like botnets monetized by cybercriminals (*RSOCKS*)



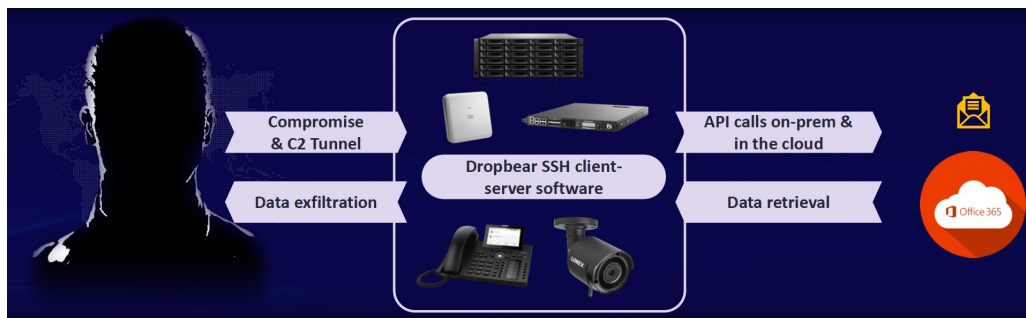
Physical attacks: Spying, attacks on power, HVAC, & devices that control physics - often associated with nation-states (*FRONTON*)



OEM attacks: Malicious xIoT assets out of the box (*Huawei, ZTE, Hikvision, Dahua & Hytera*)



Pivot attacks: Gain access through an IT asset, hide on multiple xIoT assets, attack IT assets, & exfiltrate data through the xIoT assets (*QUIETEXIT*)



HACKING

Industrial Robots




HIGH TECH

COMPANY PROFILE

- High Tech
- IoT – device development engineering

KEY FACTS

- 30 FTE's
- Scale-up
- Cybersecurity part of IT

KEY REQUIREMENTS

- CRA – Cyber Resilience Act analysis
- SBOM development
- US-based customers – compliance requirement for export

PROPOSITION

- Software Code Analysis result transposition into SBOM
- Assessing high level vulnerabilities
- Demonstrating additional vulnerabilities
- Dependency tracking
- Developing and supporting publications of SBOMs



Impact of Legislation : 1) Europe Cyber Resilience Act (09/22)



European
Commission



CYBER RESILIENCE ACT

New EU cybersecurity rules ensure more secure hardware and software products

#DigitalEU #SecurityUnion #Cybersecurity

#SOTEU
2022

SEPTEMBER 2022

The banner features a dark blue background with a circular inset on the left showing a person's hands typing on a laptop with glowing blue padlock icons. The text is in white and yellow. The European Commission logo is at the top center. The hashtag #SOTEU 2022 is on the right, and the date SEPTEMBER 2022 is at the bottom right.

A first ever EU wide legislation of its kind: the **Cyber Resilience Act** introduces **mandatory cybersecurity requirements for hardware and software products**, throughout their whole lifecycle.

Impact of Legislation : 2) US Executive Order (2021)

CYBER RISK MARCH 25, 2021 / 9:24 PM / UPDATED A MONTH AGO

Exclusive: Software vendors would | disclose breaches to U.S. government under **The Minimum Elements Bill of Materials (SBOM)**

By Joseph
Topics: [Internet Policy](#) [Internet Policy Task Force](#) [Cybersecurity](#)
July 12, 2021

Figuur 14 : htt

The Executive Order (14028) on Improving the Nation’s Cybersecurity directs the Department of Commerce, in coordination with the National Telecommunications and Information Administration (NTIA), to publish the “minimum elements” for a Software Bill of Materials (SBOM). This report builds on the work of NTIA’s **SBOM multistakeholder process**, as well as the responses to a request for comments issued in June, 2021, and extensive consultation with other Federal experts.

An SBOM is a formal record containing the details and supply chain relationships of various components used in building software. In addition to establishing minimum elements, this report defines the scope of how to think about minimum elements, describes SBOM use cases for greater transparency in the software supply chain, and lays out options for future evolution.

The Minimum Elements For a Software Bill of Materials (SBOM)

**Pursuant to
Executive Order 14028
on Improving the Nation’s Cybersecurity**



COMMERCE

COMPANY PROFILE

- Retail
- Textiles – Customized shirts on the web

KEY FACTS

- 5 FTE's
- 20+ years in operations
- Connecting to suppliers for designs and production

KEY REQUIREMENTS

- 3rd party hosting (Managed Service Provider)
- No internal IT (no cybersecurity)

PROPOSITION

- External Websites analysis – Essential Security improvements
- Support (advisory) with external hosting company – MSSP service
- API – integration analysis and vulnerability assessment
- API security hardening
- Website platform hardening



ALSO WATCH OUT FOR FSTP CYSSDE

- Up to 200k EUR for pen-testing and vulnerability assessments of SMEs, critical infrastructure and applications and devices for critical infrastructure and security
- Together with the Member State NCCs
- Joint methodology development of assessments and capacity building
- First Open Call expected to be launched before the end of 2024



Not the end



More information, slides and follow-up
www.cyssme.eu
www.lsec.eu

Q or C
Ulrich Seldeslachts
ulrich@cyssme.eu
+32 475 71 3602



© CYSSME - LSEC, 2024, Private & Confidential - Closed User Group Distribution - Do Not Distribute -
This project has received funding from the European Union's Digital Europe Programme under grant agreement No 101128101





CYSSME offers cybersecurity services for European micro, small and medium-sized businesses up to 250 employees or 50m euros in consolidated turnover.

cysme.eu

