Cybersecurity 4.0: results of survey on cybersecurity needs of manufacturing companies

28 March 2023, 16:41

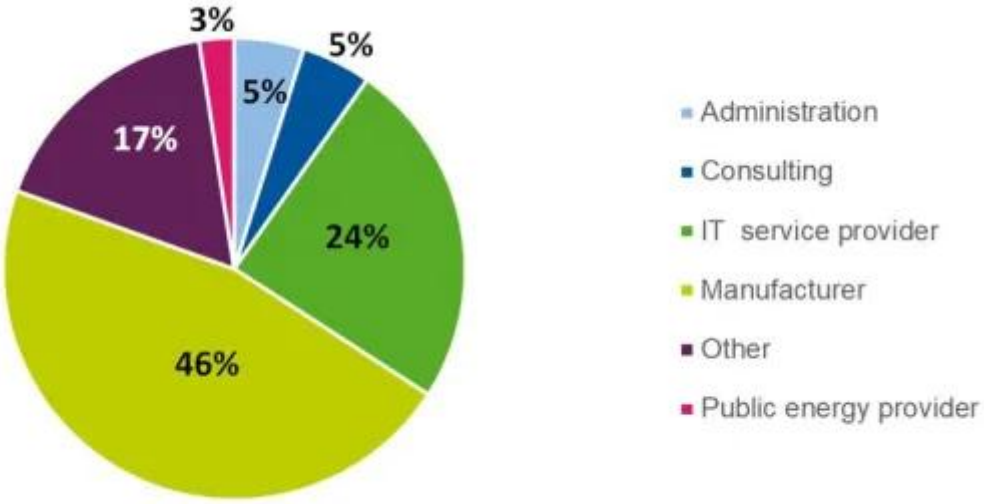
Tatiana Galibus
Annanda Rath

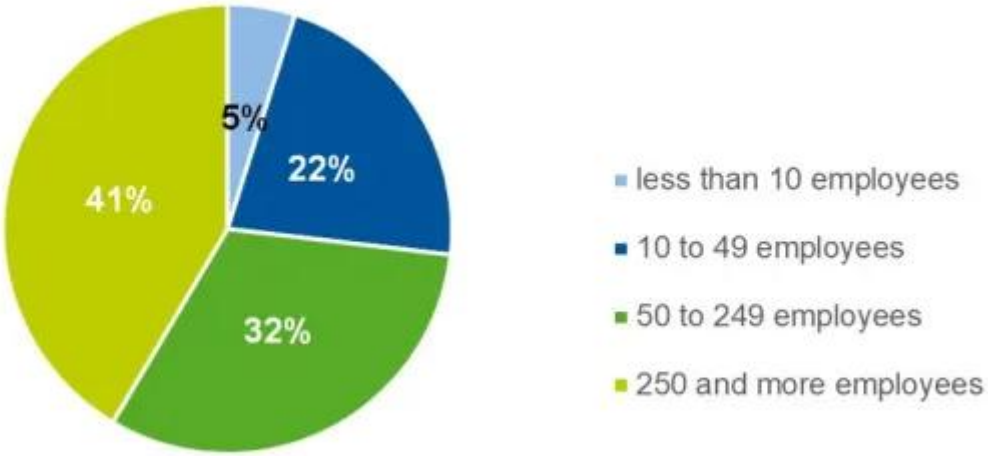
From March to October 2022, we conducted a survey with manufacturing companies from Belgium and Germany, within the context of the research project Cybersecurity4.0. You can find some interesting results and tendencies from the survey in this blog post.

Cybersecurity 4.0 is a research project with the ambition to propose to SMEs a feasible cybersecurity framework and learning environment, with focus on connectivity, data and supply chain security.

Analysis of test cases and user requirements

41 companies were interviewed or surveyed.





We have analysed the results of the survey, using a statistical classification, scoring and rating methodology. As a result of the survey, we have identified **3 basic company profiles**: manufacturing company, SME and service provider. We identified **11 important security domains** to be taken into account by companies, while implementing cybersecurity, among which are: network and data security, supply chain security, access control and OT/IOT security, etc.

Security risks for manufacturing companies

We identified t**he highest security risks** for manufacturing: we observed that there are security deficits in many critical security domains, most of which are in access control monitoring, data classification, cybersecurity training and security assessment for the supply chain partners. Among the 20 (or 46%) companies that were interviewed and have answered the online survey: 13 companies do not classify their data, 11 companies do not audit the access to their system and network and 8 companies do not protect their backup with encryption. More than 50% of companies (12) do not assess security risk in their supply chain partners and 10 companies do not have cybersecurity training programs, which is considered as an important factor for cybersafe practice.

Deficit	Frequencies	Comments
No back up encryption	8	+ 1 "Not specified" + 1 "Don't know"
No access control	5	-
No audit of access control	11	+ 1 "Don't know" + 1 "Not specified"
No data classification	13	+ 1 "Not specified"
No network segmentation	5	+ 2 "Don't know"
No network monitor	6	+ 1 "Don't know"
No cyber security training	6	-
No implementation standards for cyber security training	10	+ 2 "Don't know" + 7 "Not specified"
No risk assessment for supply chain partners	12	+ 2 "Don't know"

Table 1. List of security deficits in manufacturing companies interviewed

Security risks for service provider companies

For service provider companies, we see a relatively improvement in terms of security deficit. However, there are still some security deficits in critical domains, such as access control, data classification and security assessment of their supply chain partners. 5 out of 10 (or 24%) companies still do not have a proper access control system or best practices, and 7/10 do not have security risk assessment for their supply chain partners. 4 companies do not have a cybersecurity

Deficit	**Frequencies**	**Comments**
No backup encryption	1	+ 4 "Not specified"
No access control	5	+ 1 "Not specified"
No audit of access control	5	+ 1 "Not specified"
No data classification	5	+ 1 "Don't know" + 1 "Not specified"
No network segmentation	2	+ 1 "Not specified"
No network monitor	3	+ 2 "Not specified" + 1 "Don't know"
No cyber security training	4	
No implementation standards for cyber security training	4	+ 4 "Not specified" + 1 "Don't know"
No mitigation plan	4	+ 2 "Not specified"
No risk assessment for supply chain partners	7	-

Table 2. list of security deficits for service provider companies

Security risks for SMEs

59% of the 41 companies we surveyed and interviewed are SMEs (i.e. companies with less than 250 employees). We see a similar trend concerning the security deficit ranging from access control, data classification, network monitoring, cybersecurity training and mitigation plan and security risk assessment for supply chain partners.

Deficit	Frequencies	Comments
No backup encryption	-	+ 1 "not specified" + 1 "don't know"
No access control	3	+ 1 "don't know"
No audit of access control	4	+ 1 "don't know"
No data classification	4	+ 1 "don't know"
No network segmentation	4	-
No network monitor	2	+ 1 "don't know"
No cyber security training	3	-
No implementation standards for cyber security training	3	+ 2 "not specified" + 2 "don't know"
No mitigation plan	2	+ 2 "don't know"
No risk assessment for supply chain partners	4	+ 1 "don't know"

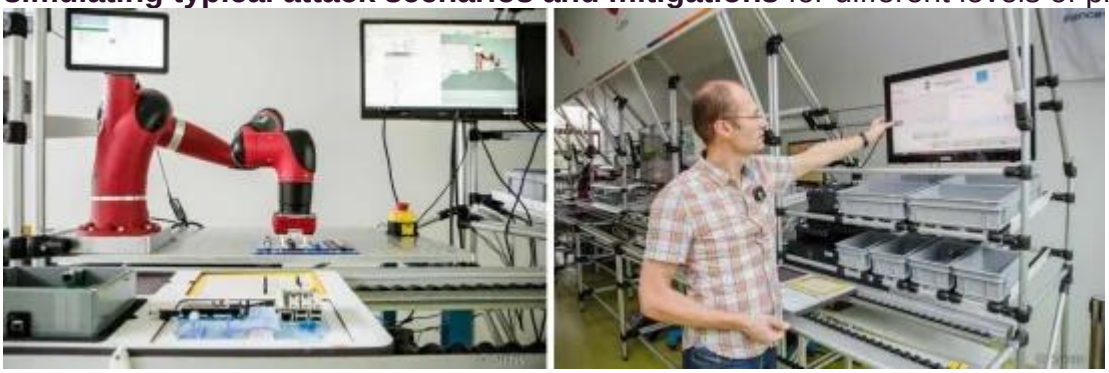
Table 3. list of security deficits for SMEs

Specification of maturity model, vulnerability and risk analysis

Currently, we are in the process of specifying the criteria of cybersecurity maturity in relation to company profile and risk. We shall be able to classify the companies per cybersecurity levels 1-4

In April, Sirris and FIR Aachen will publish the questions of the survey, so that any company will be able to answer them online.

As a next step, we shall develop a **framework, web tool and guideline**s as a future web platform supporting cybersecurity. A **demonstrator** will be implemented as a connected production line **simulating typical attack scenarios and mitigations** for different levels of protection, including



Together towards Cybersecurity 4.0

The goal of the Cybersecurity 4.0 project is to develop tools for awareness and dissemination. Are you interested in a particular topic of cybersecurity, would you like to have a closer look at results or set up a call with us or with other Belgian companies? Contact us!

At the **end of April** we will organize an online Belgian consortium meeting, a webinar for the user group or to answer your specific question or concerns.

On **27 April**, Sirris launches a 2-months education trajectory with a hands-on practical focus to help manufacturing companies with cybersecurity: join us!

Also, we offer individual coaching sessions and masterclasses on your premises, in order to help you design your own cybersecurity strategy and eliminate specific risks. Check our collective and individual offerings!

Authors

Tatiana Galibus

Annanda Rath