Report: Results of Simulation-based Competence Development Survey (2019-2020)

- A collaboration between the European Cyber Security Organisation (ECSO) and the European Cybersecurity Competence Network Pilot projects

Contents

1 Introduction

This paper provides the key findings and results from the analysis of simulation-based competence development around cybersecurity in Europe, based on survey responses received over the course of two months (Sep-Nov 2019). This analysis on simulation-based competence development in Europe is a collaboration between the working group (WG5) for competence building at the European Cyber Security Organisation (ECSO) (https://www.ecs-org.eu) and the Cybersecurity Competence Network (https://cybercompetencenetwork.eu).

Established in 2016, the European Cyber Security Organisation (ECSO) is a non-lobby association that is engaged in a contractual Public-Private Partnership on cybersecurity with the European Commission. Thanks to its large membership network from all across Europe which includes national and regional public administrations, large companies, SMEs, research centres/academia, associations and users/operators, ECSO is in a privileged position to cover the various aspects of cybersecurity R&I and industrial policy with the intention of building a comprehensive approach for strengthening the cybersecurity ecosystem in Europe. This includes various activities on education, training and awareness in its WG5, where cyber ranges and simulation-based competence building has been a key topic for its members over the past two years.

The four pilot projects (CONCORDIA, ECHO, SPARTA and CyberSec4Europe) have been chosen to address the Horizon 2020 Cybersecurity call “Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap”. The collaboration of these four pilot project consortia of over 160 partners establishes the foundation of the European Cybersecurity Network and Competence Centre.

The following work is spearheaded by ECHO, with the support of ECSO.

2 Simulation-based Competence Development Study by the European Cyber Security Organisation (ECSO) and the Cybersecurity Competence Network

The overall purpose of the survey was to assess how organisations in Europe currently address competence development through simulations, exercises etc. in order to understand how to deliver solutions better fitting the needs of European organisations in raising cyber resilience. With the understanding of these needs and requirements, the European Cyber Security Organisation and the participating network of Cybersecurity Competence Centres will be able to deliver solutions and recommendations that will have a long-lasting effect on securing the European cyberspace.

The data for the “Simulation-based Competence Development Study” was gathered through an online survey which took place from September until beginning of November 2019. The survey results are presented in the following analyses.

The number of respondents was limited, given the short timeframe, which naturally affects the representativeness and validity of results. Nevertheless, the responses provide an initial overview of the situation and the following analysis also includes additional findings from roundtable discussions organised by the ECHO project. In addition, it should be noted that not all respondents were willing to share their information due to confidentiality, competition or because they did not consider the questions relevant to their business (motivation). Nevertheless, open-ended qualitative questions of this survey provide important information about their current services and potential needs. This analysis is completed in collaboration between five organisations or networks, and their respective authors are responsible for the content.

3 Analysis and Results

3.1 Background of the Respondents

The number of respondents amounted to forty-three (n=43), and their positions varied from student to director from forty (40) different European organisations. The respondents were developers, architects or engineers (n=9), managers (n=7), directors (n=5), experts, researchers or analysts (n=5), security officers (n=4), coordinators or experts (n=4) advisors or consultants (n=2) and professors (n=2). They represented mainly private organisations (74% of the respondents) or public organisations (26% of the respondents.

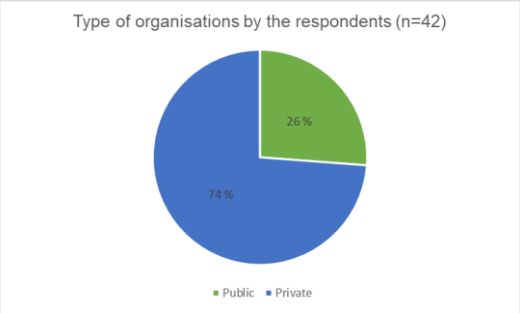

Figure 1 - Type of Organisations

The organisations that the respondents represented were medium or large size organisations (over 50 employees). 56% (24 out of 43) replied that their organisation employs more than 250 employees. There were no organisations with less than five employees who responded to this survey.

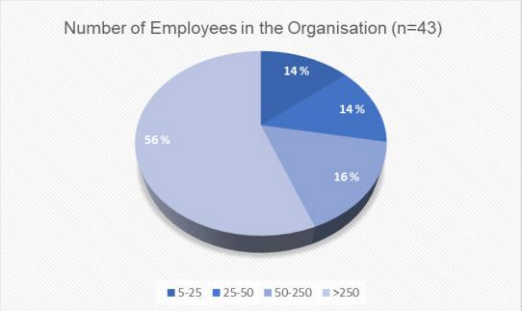

Figure 2 - Number of Employees

Most of the respondents reported having an in-house IT/cybersecurity team (83%) while 51% have a dedicated C-level IT security position with an additional 25% where the IT/Cybersecurity team report to the Head of IT. In smaller companies (less than 250 employees) it is also common that

the IT/Cybersecurity team is reporting directly to Managing Director or CEO (14% of all respondents)

Out of the 43 respondents, 22 have mandatory compliance requirements with another 13 expecting to have such requirements soon, with most of the large organisations (more than 250 employees) in those categories.

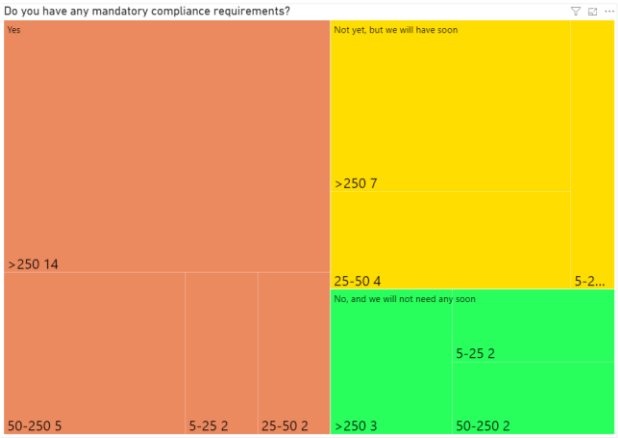

Figure 3 - Compliance requirements per size

3.2 Addressing cyber issues in organisations

3.2.1 Importance of cybersecurity

The majority of the respondents (40 out of 43) described cybersecurity as a “very important” or “important” thematic topic to their organisations. Six respondents elaborated that cybersecurity is not important for their organisations Others responded that they thought it is important and should be addressed more in detail in their organisation.

When asked to elaborate on the importance, the respondents answered, *"We have dedicated in-house competence and capability building programmes"* (n=28), *"We conduct regular in-house vulnerability assessments"* (n=27) and *"We use security as an enabler (maintaining proper cyber hygiene and security measures positively affects business processes)"* (n=24) as the most crucial reasons for the importance. Some respondents identified the reasons *"We conduct regular vulnerability assessments by external providers"* and *“We have out-sourced partners for handling cyber attacks"*. When we analyse the types of measures taken against the size of the organisation (illustrated on the figure below), as expected, in the larger organisations we see dedicated teams, regular vulnerability assessment and using security as an enabler. However, those are also employed by much smaller organisations (5 to 25) and the only negative answer “We don’t address it” was given by an organisation with more than 250 employees. It seems there is currently no

clear difference on the various actions taken by organisations based on their size, but decisions are based on security maturity or other factors.

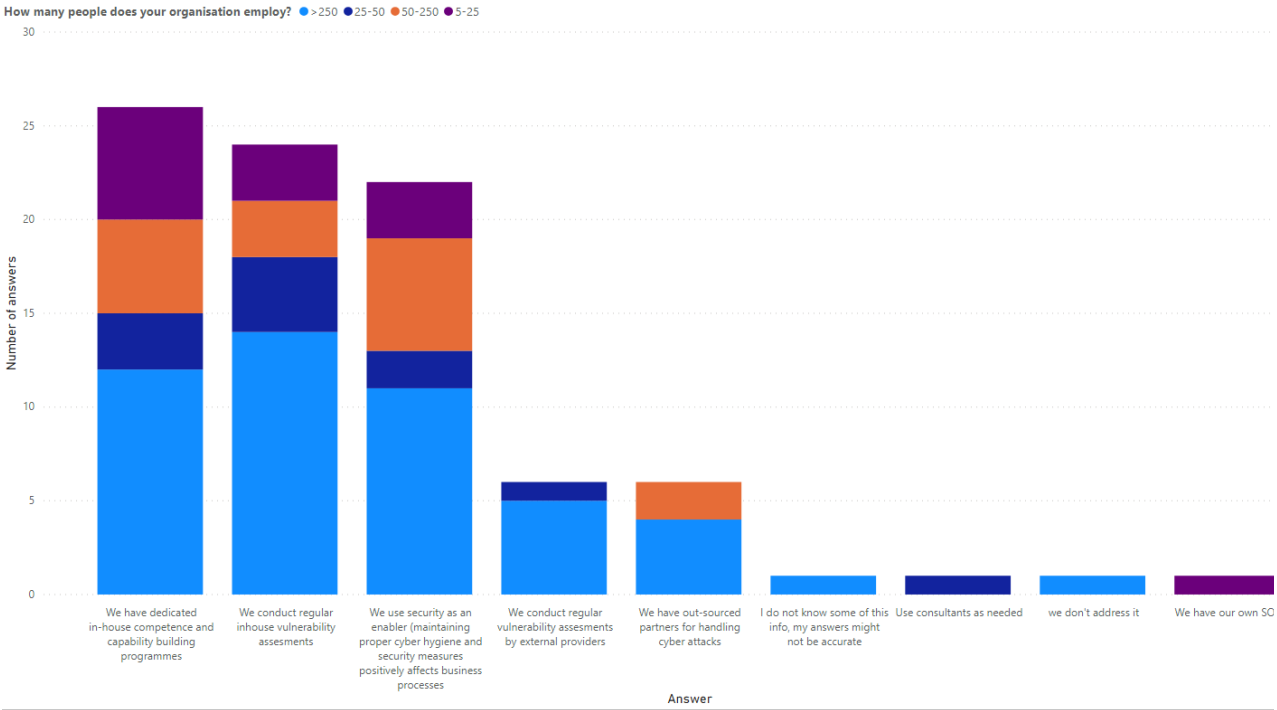

Figure 4 - Importance of Cybersecurity in the Organisation

3.2.2 Organisational Cyber Capabilities

Only 48% of the respondents answered that their organisation has IT security compliance certification (ISO, CC, CoBit, etc). 59% (26 out of 43) of the respondents replied that their organisation does apply security measures, using the response “during the planning process we cultivate the security/privacy by design principles”. Moreover, 24% clarified that they “react to situations when they occur”. In terms of hiring new personnel, respondents consider the relevant educational background and work experience the most important. Only 16% (7 out of 41) ask for MSc/BSc and certain industrial certifications (SANS, EC, etc). Expectedly, the larger organisations (with more than 250 employees) are more likely to have some kind of certification, but a number of organizations with between 25 and 250 employees are in the process of obtaining such certification, which means that in the current environment smaller companies can benefit from certification.

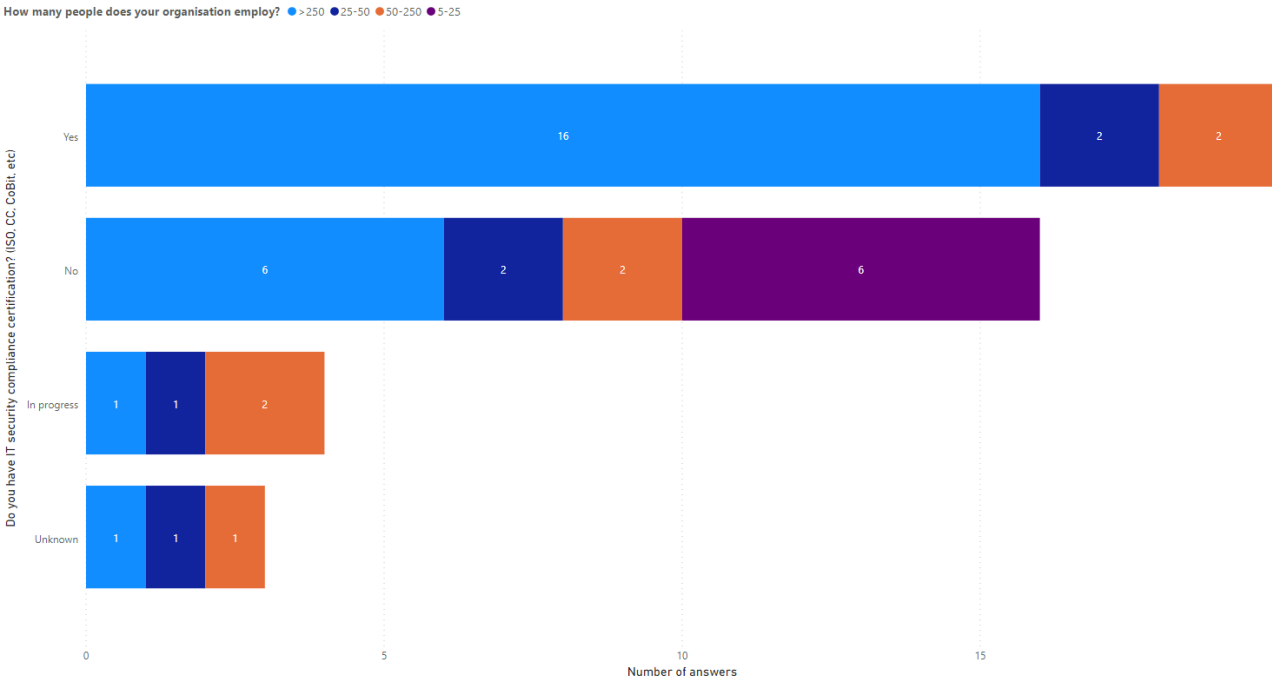

Figure 5 - Do you have IT/cyber security compliance certification?

Examining the private/public company distribution on the same questions, it can be confirmed that more and more private companies can draw benefits from certification.

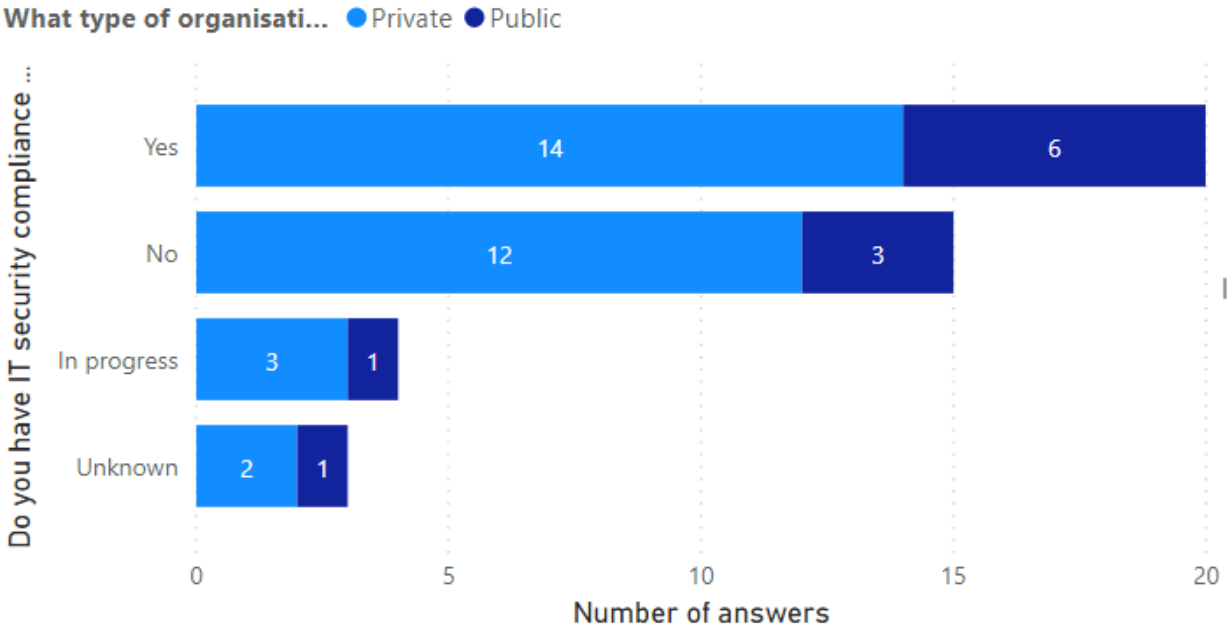

Figure 6 - Certification and organisational type

3.2.3. Budget dedicated for cybersecurity

The budget that respondents' organisations have dedicated to cybersecurity was also surveyed. 67 % (27 out of 41) of the respondents replied that their organisation has budget dedicated for cybersecurity activities. 28 % (11 out of 41) of the respondents answered that the dedicated budget is planned on a yearly basis, and only two answered there was no budget dedicated for cybersecurity.

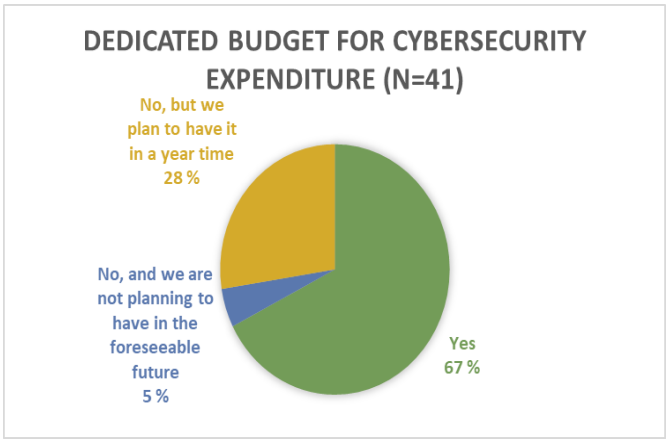

Figure 7 - Dedicated Budget for Cybersecurity by the Organisation

3.2.4. Employee Competences and Skillsets

When it comes to the hiring process, a majority of organisations reported that they check the educational background and work experience of candidates (62%) with only 16% asking for BSc or higher education.

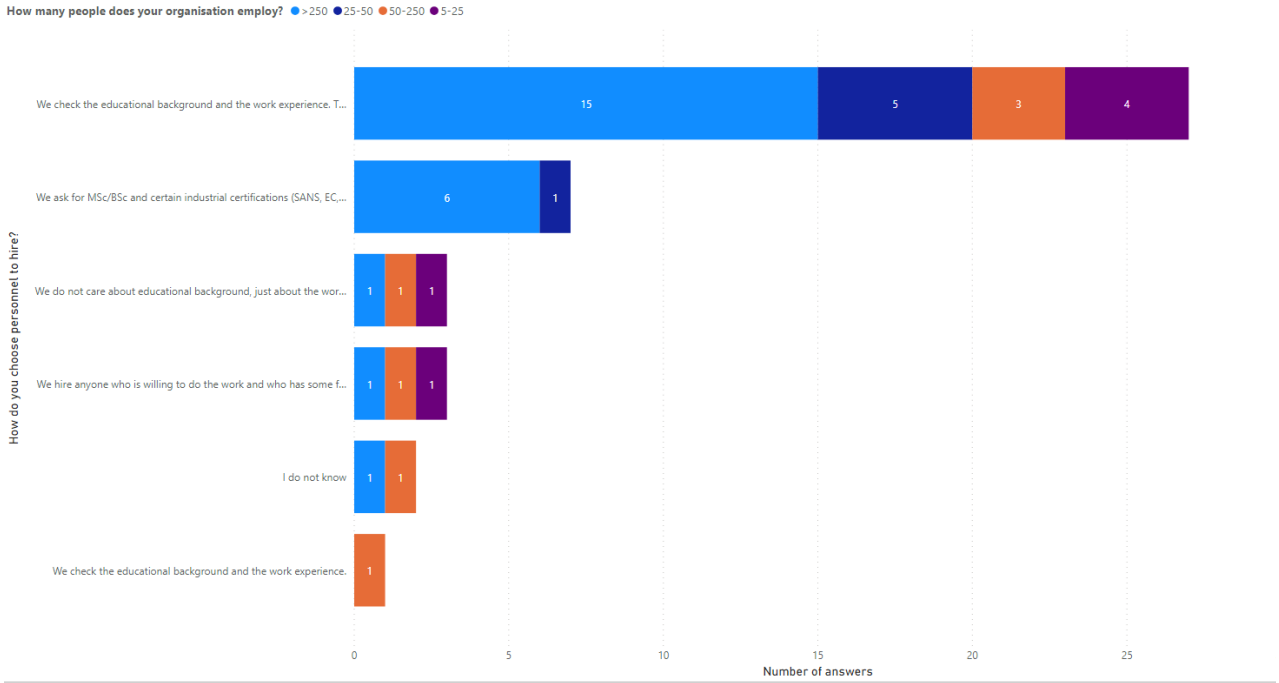

Figure 8 - Employee Competences and Skillsets

There does not seem to be a clear separation in hiring practices between large and small companies and a majority of organisations (81%) will hire someone without a degree but with proven competence. This applies to small and large organisations alike and demonstrates that very often in the field of cybersecurity people are hired based on competence and proven track record, regardless of their education.

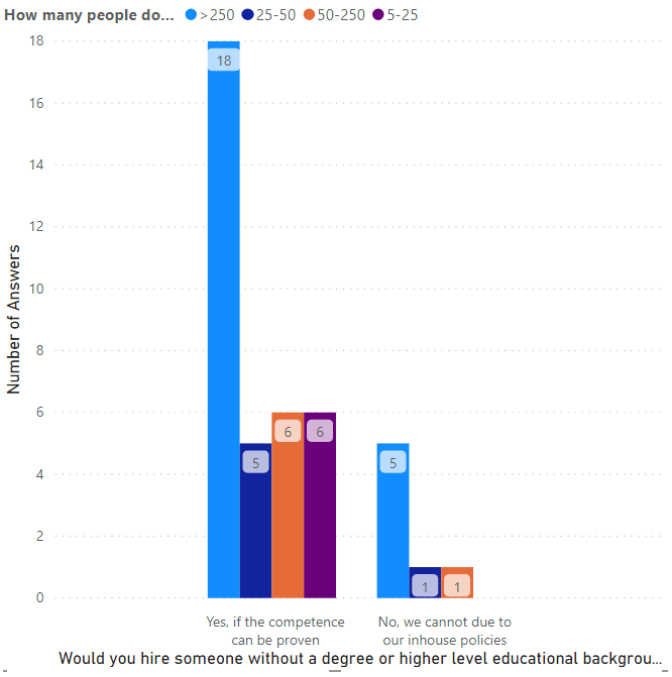

Figure 9 - Competence vs education

The respondents were asked about dedicated career planning by the organisations for the employees. 44% of the respondents (19 out of 43) highlighted that they have an in-house roadmap for employees currently in place. Only 7% responded that they do not have planning of career paths and they do not plan to have it. 76% of the respondents said they currently run cybersecurity trainings available for their employees.

Expectedly, in the majority (13 out of 24 respondents) of large (>250 employees) organisations, there is an inhouse roadmap. Smaller organisations are focusing either on planning a career path roadmap or are supporting the progression by financing trainings and other activities. Less than 1% of respondents said that they do not have career path planning.

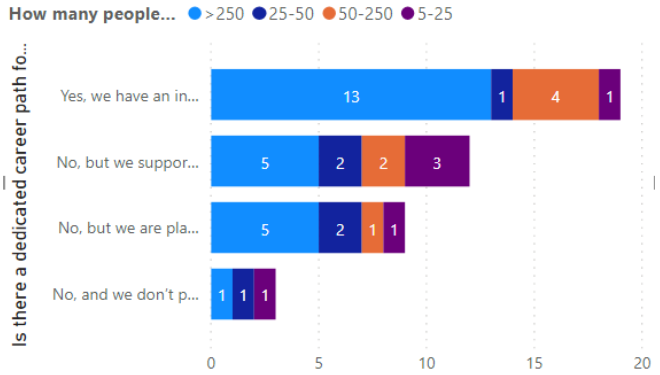

Figure 10 - Career Path for Employees

When analysing the responses on the survey question "*How do you know which competences are missing from your organisation?*", over half (22 out of 41) replied that they conduct

assessments regularly to understand the various skillsets and focus on development based on that. The rest of the respondents use traditional “wish lists” for the employees, where they ask their employees what they wish to learn and arrange trainings based on that (or they guess).

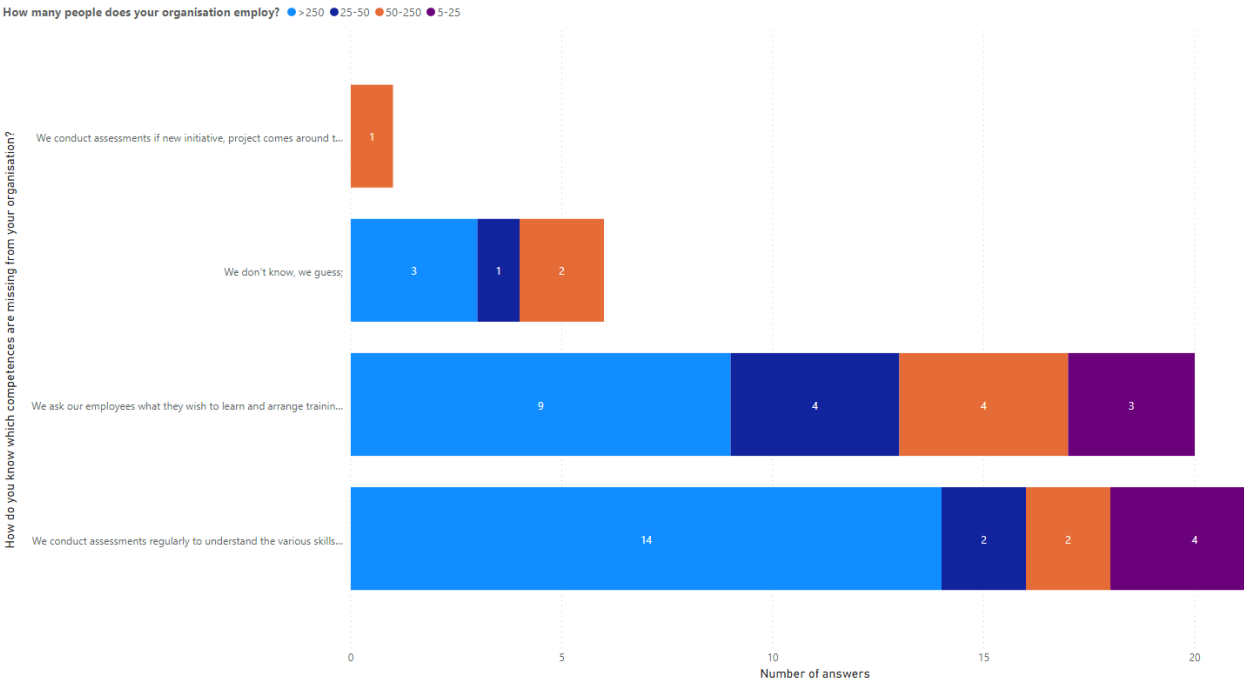

Figure 11 - Understanding Missing Competences

As is visible on the above graph, the survey indicates that smaller organisations are actually better at understanding the missing competencies as virtually all of those between 5-25 employees either regularly asses or reach out to employees.

When asked about “*How do you measure competence building efficiency?”,* a majority of the respondents (16 out of 42) valued conducting assessments regularly to understand skillsets and how to develop them. In addition, linking cyber exercises and learning from the results was addressed as a highly important practice. When analysing the distribution of answers related to the size of an organisation, no clear trend could be identified separating smaller organisations from larger ones.

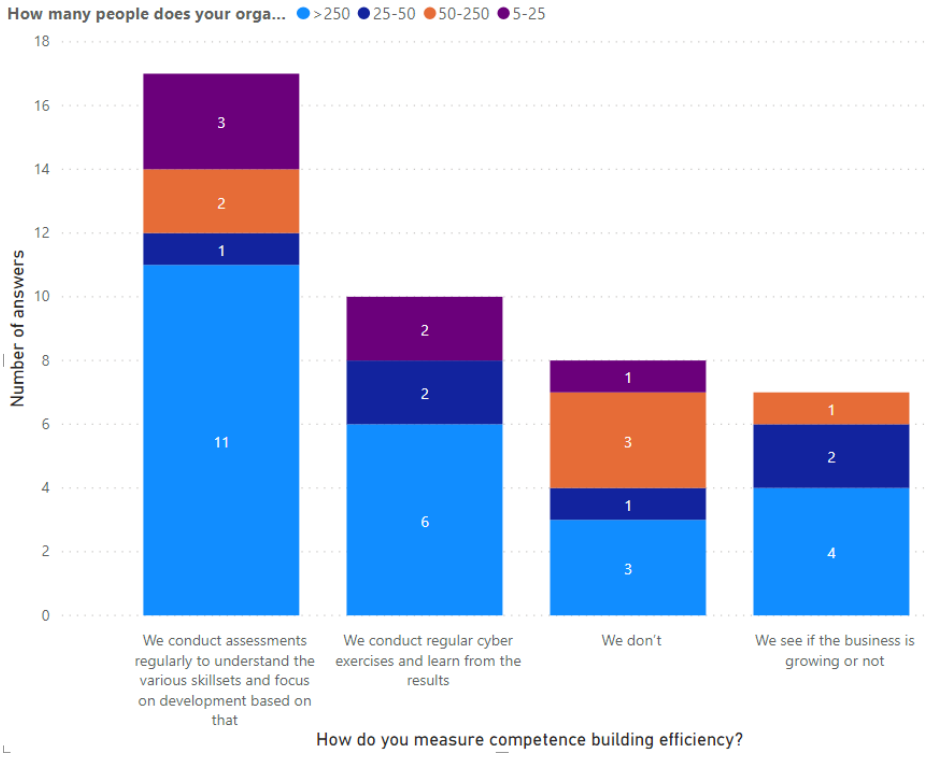

Figure 12 - Measuring Competence Building Efficiency

When asked, "*How do the organisations measure cost effectiveness of cybersecurity expenditures?*" 54% (22 out of 41) answered they do not measure the cost effectiveness at all. The rest of the respondents indicated that they either have *historical data mapped against potential cyber threats and make decisions based on the analyses* or that *they have a fixed budget to spend each year, regardless of what the threats are*. Also, there was a specific question about the allocation for cybersecurity training for the staff of the organisation. Over half of the respondents replied that they use *less than 20% of* organisational turnover for cybersecurity capacity building purposes. Almost 10% of the respondents don't know how much of the turnover goes to capacity building purposes and 6 out of 41 (15%) are spending more than 20% which leads to the conclusion that the respondent group contains cybersecurity specialised companies.

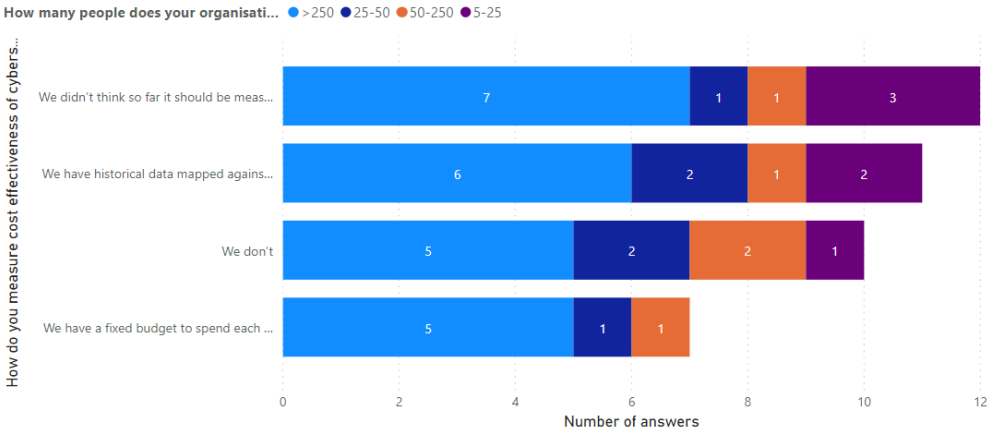

Figure 13 - Measuring Cost Effectiveness

3.2.5 Preparation and mitigation of vulnerabilities by organisations

A majority of the organisations 70% (28 out of 41) responded that they do participate in full-scale vulnerability assessments every year. 10% (4 out of 41) had an assessment more than a year ago and 20% (8 out of 41) of the respondents addressed that they have never completed a full-scale vulnerability assessment. Overall, 80 % of the respondents replied that their organisations have had full-scale vulnerability assessments.

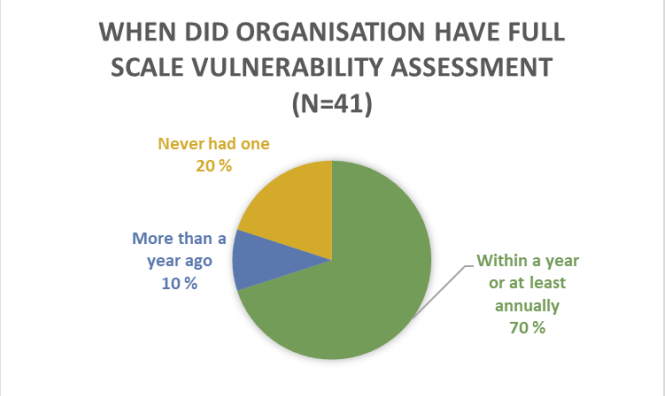

Figure 14 - Full-scale Vulnerability Assessment

In order to respond to needs and threats, the rise of cyber resilience is identified as a key activity. The respondents were asked about how they know that they are investing in the right tools and practices to raise their cyber resilience. 20 out of 41 replied that they trust their own assessments ("we know our needs based on our self-assessment and purchase products accordingly"). Only 7 out of 41 elaborated that they see cyber exercises as key metrics to identify correct tools and practices ("we regularly have cyber exercises to define the level of corporate resilience and identify key milestones for improvement").

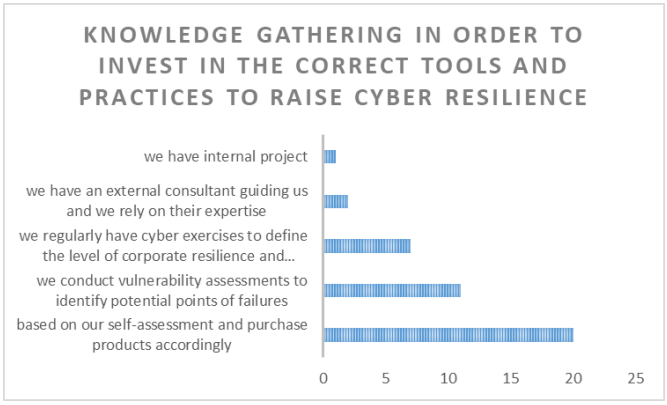

Figure 15 - Knowledge Gathering

If the size of the organisation is considered, small organisations (5 to 25) are focusing on self-assessments with just one respondent conducting vulnerability assessments. Cyber exercises appear to be more in the territory of larger organisations (6 with more than 250 employees and one with between 25 and 50).

The survey had a specific question about organisations having financial vehicles to mitigate potential cybersecurity risks. A majority of the respondents (61%) clarified that they do not have financial vehicles to mitigate risks for various reasons. Yet, they said that they are considering having financial vehicles. Also, some replied that they are not aware of what financial vehicles actually are. If respondents elaborated positively, they specified that they use cyber insurance to cover certain types of incidents.

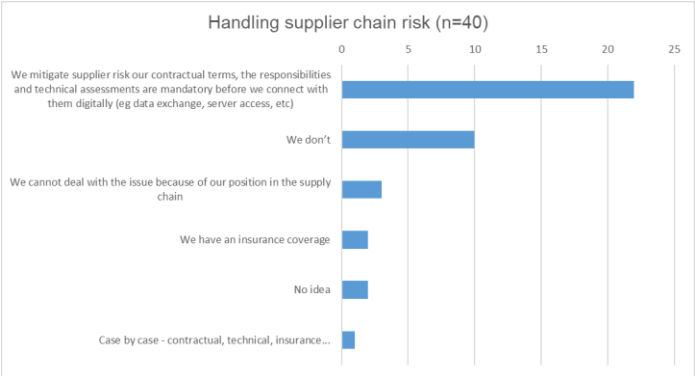

Figure 16 - Handling Supplier Chain Risk

In terms of mitigation, the survey included a question about handling supplier chain risk. A majority of the respondents addressed as a key mitigation process towards the risk; "*We mitigate supplier risk our contractual terms, the responsibilities and technical assessments are mandatory before we connect with them digitally (e.g. data exchange, server access, etc*)". The other practices varied or there was no clear practice to handle supplier chain risks in the organisation.

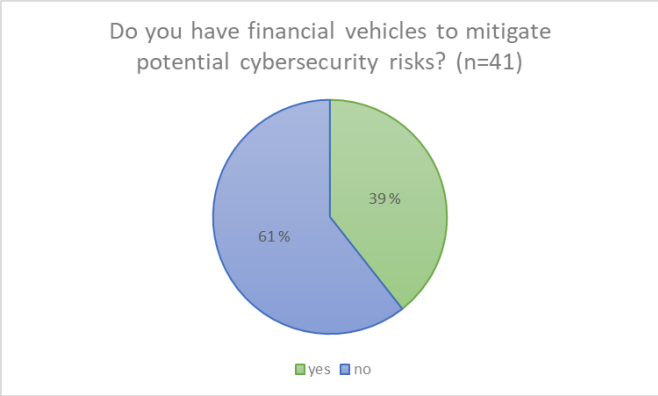

Figure 17 - Financial Vehicles to Mitigate the Risks

3.3 Simulation-based Competence Development: Cyber Ranges

3.3.1 Familiarity with the terminology

Respondents were also surveyed on their familiarity with the term “simulation-based competence building”. Over half (55%) felt familiar with the definition. 95% (41 out of 43) of the respondents were familiar with the definition “cyber range”, but less than half of those admitted that they use cyber ranges regularly or from time to time. The graph below captures the answer distribution according to the size of organisation, where no clear difference in the approach of smaller and larger organisations can be observed.

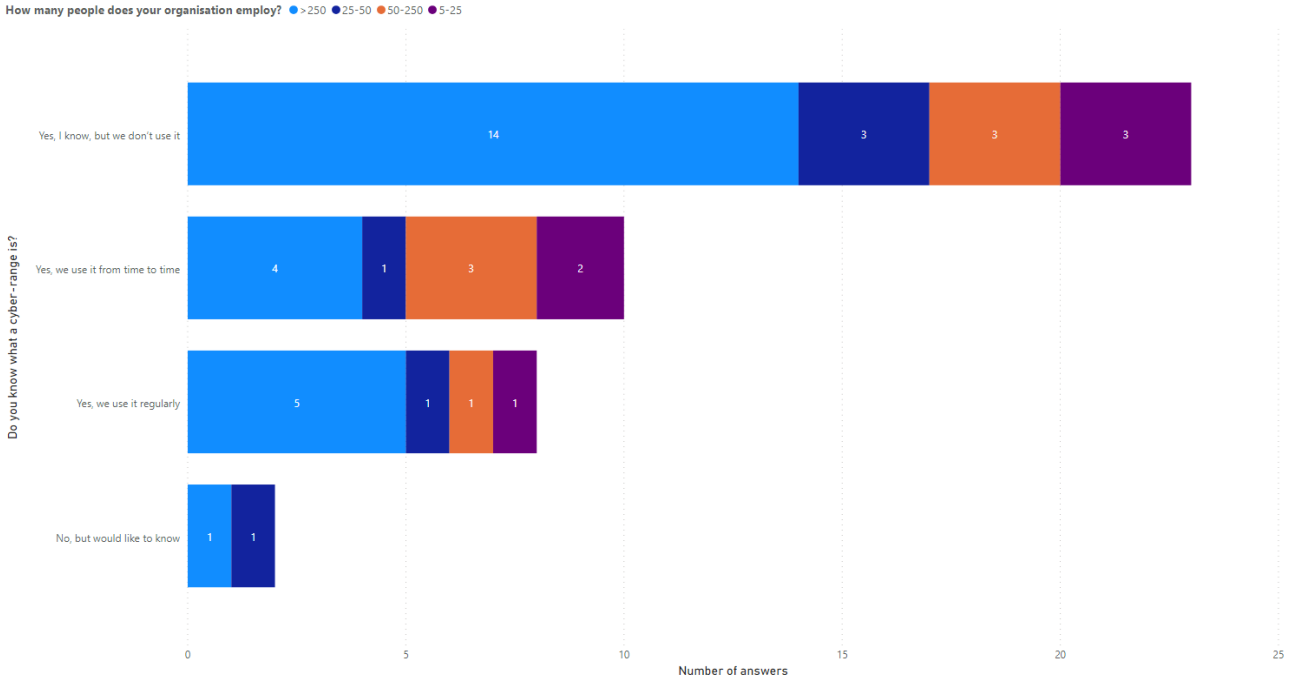

Figure 18 - Technology familiarity

3.3.2 Cyber Range Services

In relation to the survey question “What are the key features you expect from a cyber range service?”, the respondents addressed the importance of “Easy to Setup” (30 out of 41), “Plug and play contents for addressing special training needs” (29 out of 41), “Scalability” (26 out of 41) and “Highly secure” (23 out of 41) high.

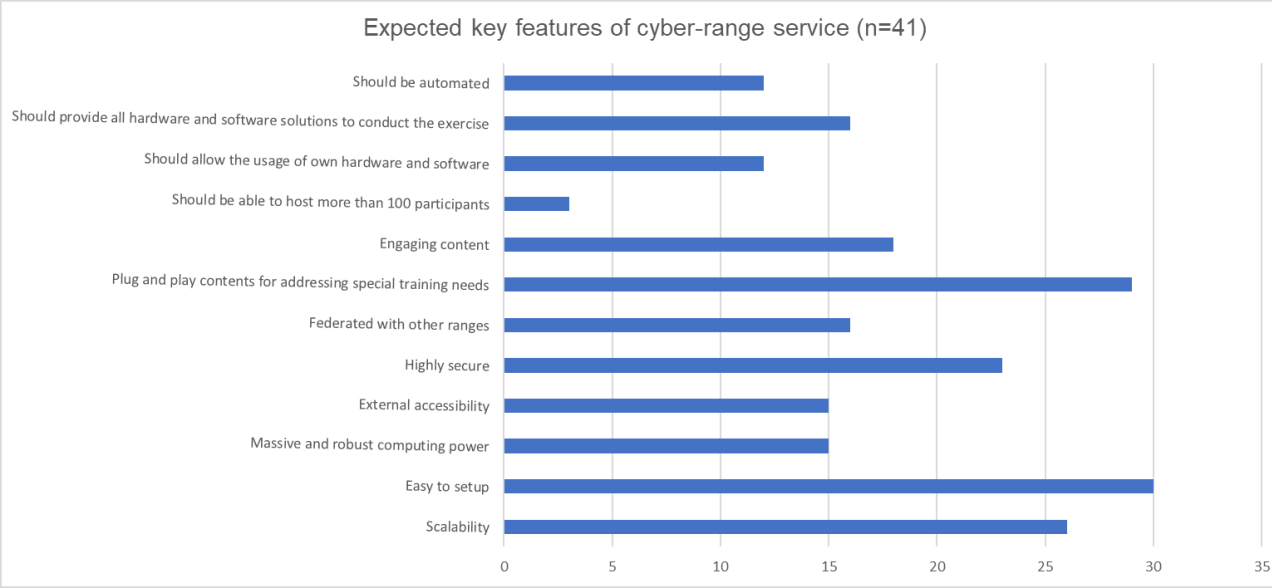

Figure 19 - Expected Key Features of Cyber-Range Service

When asked about preferred usage of cyber ranges, 58% of the respondents valued in-house training to external training service. Especially the in-house training was favoured by the organisations with a number of employees ranging from 25-50 and 50-250.

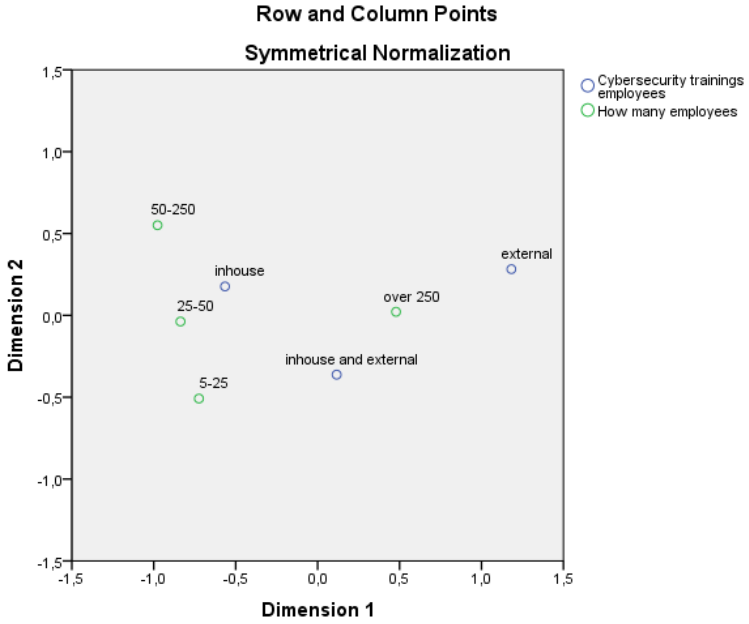

Figure 20 - Correspondence between Favoured Cyber Security Trainings and Organisations' size.

When asked if in-house of external training is preferred, 58% would choose in-house cyber range. Notably, companies with between 25 and 50 people mostly show a preference towards external providers.

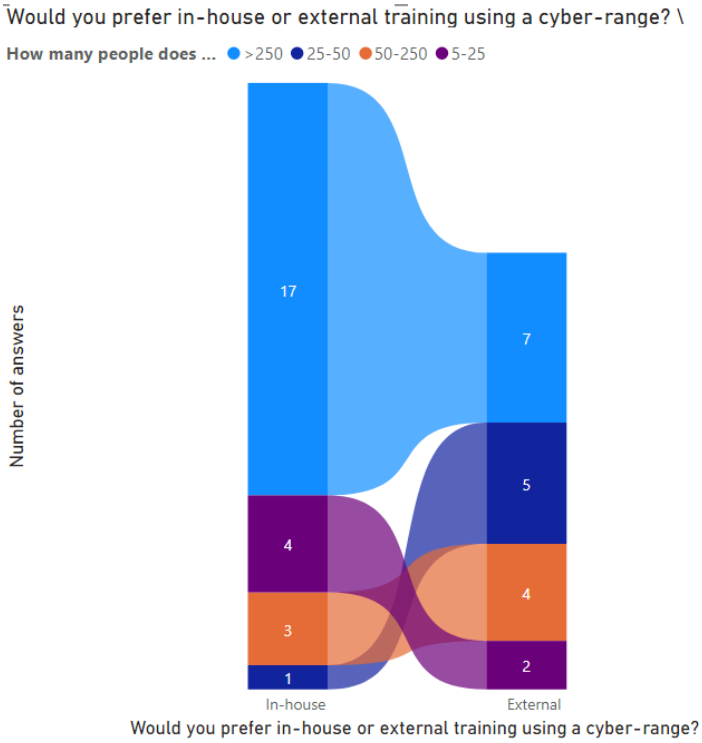

Figure 21 - In-house or external training and Organisations' size

3.3.3 Favoured Cybersecurity Providers

In the survey, the respondents provided their viewpoints on purchasing cybersecurity services from another European country. There is a clear indication that organisations were willing to purchase cybersecurity services from another European service provider if they would have a proven record of success and reputation. A few respondents replied that they have rather strict rules on purchasing from specific providers.

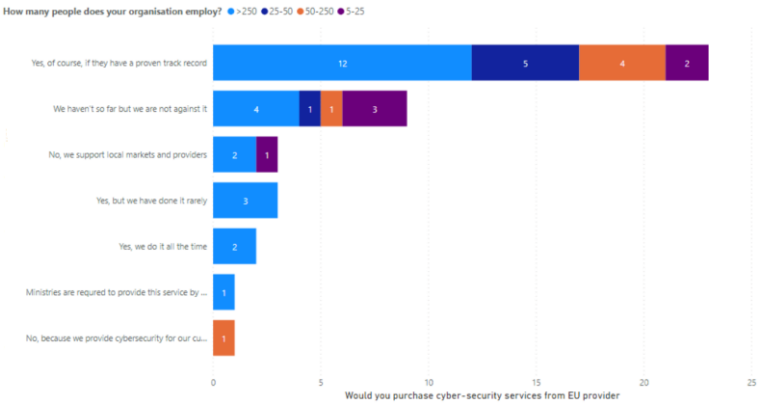

Figure 22 - Purchasing Cybersecurity Services from another European country

Only a few respondents claim that they will look for local vendors, with 21 respondents (especially organisations with up to 50 people) looking for proven track record before purchasing. It's worth mentioning that 9 organisations claimed that they are not against purchasing from the EU but

haven't done so as there might be other factors affecting the purchase, for example the fact that most of the organisations below 50 people who participated in the survey either don't have a dedicated cybersecurity budget or it's less than 10% of their turnover.

There was also an interest to see whether the respondents favour European or non-European solutions. A majority of the respondents highlighted that they would choose the European provider in case of an equally good solution. A lot of respondents also responded that they do not care about the country of origin. Some replied that they never thought about this aspect before, but rather that they look for the company profile and reputation, or that the situation is dependent on the type of product.

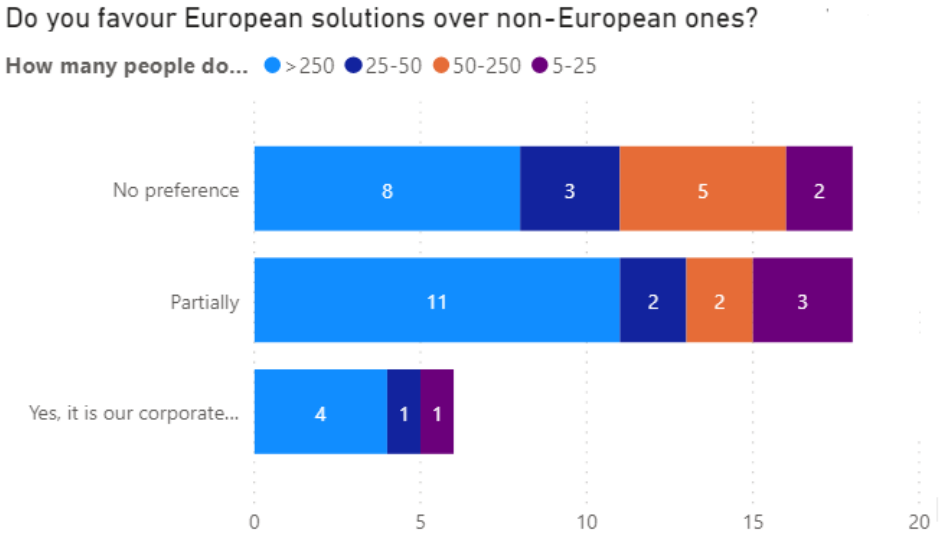

Figure 23 - Favouring European Solutions over non-European ones

With correspondence analysis (Figure 18), the differences between different sized organisations and their willingness to purchase services have been analysed. It can be observed that companies with a size of 5-25 employees purchase services "all the time" (by using Euclidean distance in correspondence analysis). The larger organisations seem to prefer any organisation with a proven track record.

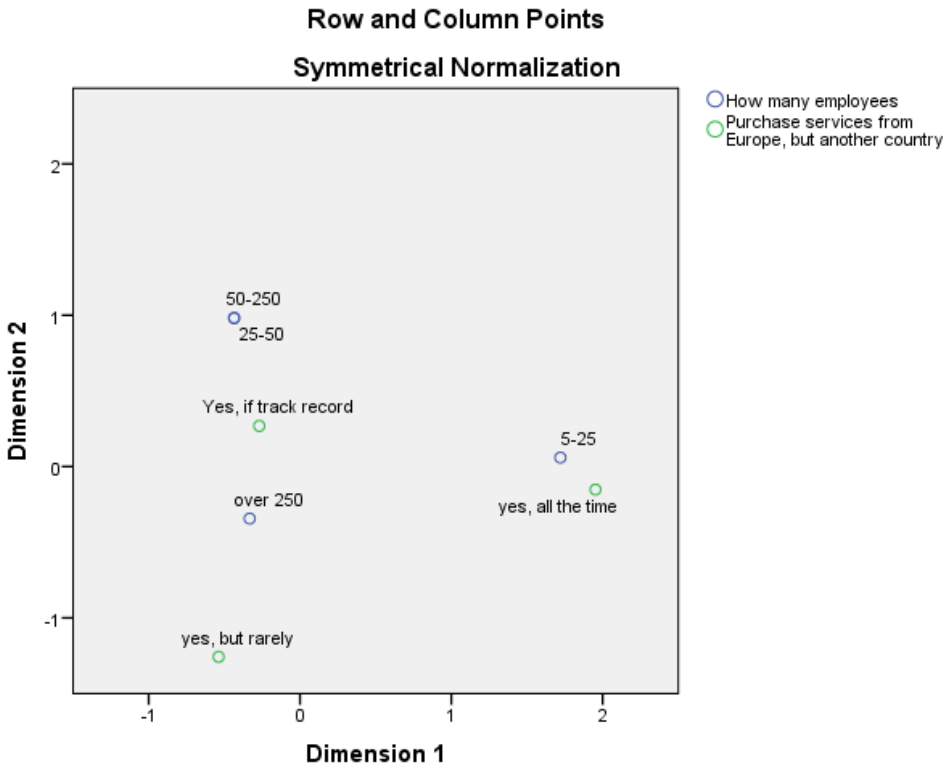

Figure 24 - Corresponding "How many employees?" and "Purchasing Services"

3.3.4 Cyber Range Design: skills and training audience

3.3.4.1 The general need to raise the level of cybersecurity

When asked about the needs from the organisations in order to build cybersecurity, the respondents provided their views based on open-ended question (qualitative analysis). 7 out of 20 respondents addressed a specific need for training or cyber ranges. A few answered that general awareness is still the most needed or missing aspect from the organisation. One respondent described that they are behind the technology developments and it is hard for the employees to keep up with the latest trends and developments. The rest of responses focused on increased data protection, lack of compliancy policies and standards, the age of the personnel and the effect on capabilities to be prepared for vulnerabilities, as well as the need to set up SOC and Early Warning Systems. One respondent described that the missing parts in relation to cybersecurity are comprehensive "*The management is changing, no time for analysing the*

vulnerabilities, too few people, small professional staff. Too old colleagues. Not real and exact definitions, lack of knowledge of good practices."

3.3.4.2 Cybersecurity skills that are demanded from the employees

The survey also asked respondents the question "*What are the key cybersecurity skills that you demand from the employees*". The respondents defined situational awareness and communication as the key skills. Moreover, collaborative, approachable as well as analytical were seen as key "skills" or desired behavioural attributes by the employees in cybersecurity.

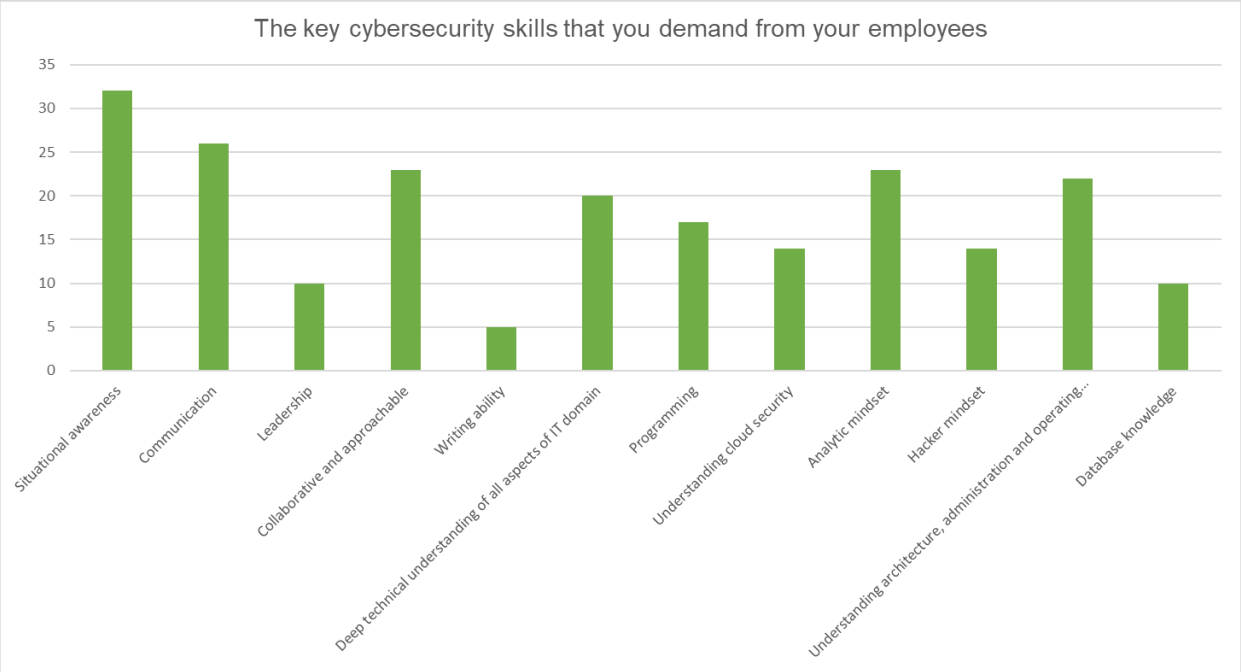

Figure 25 - Demanded Cybersecurity Skills from the Employees

3.3.4.3 The target audience for cyber range in the organisation

When asked about who should be trained using a cyber range, the majority of the respondents (21 out of 41), especially the organisations with up to 25 employees, were of the opinion that everyone in the organisation should be trained. 14 out of 41 answered that IT staff is the only personnel group to be trained with slightly more large organisations providing that answer.

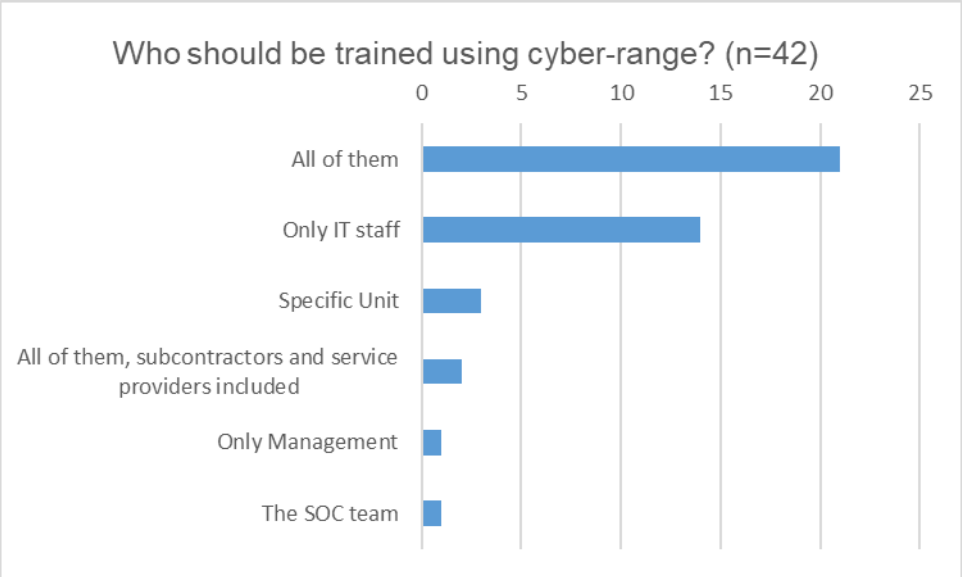

Figure 26 - Preferred Training Audience

The acceptable costs of the cybersecurity training stayed at a rather low level (0-10 % or 10-20%), in terms of proportion of the entire cybersecurity budget of the organisations.

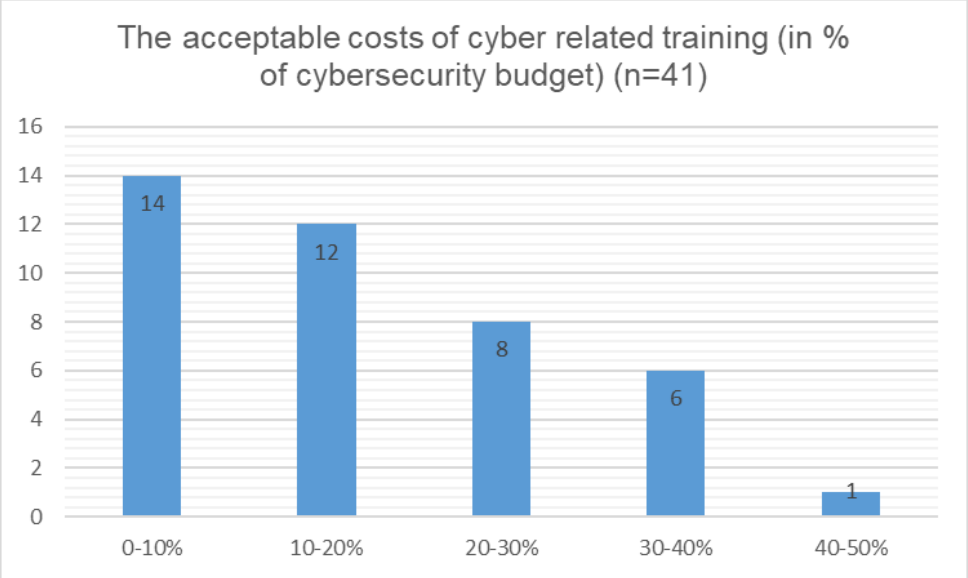

Figure 27 - Acceptable costs of Cybersecurity Training

3.3.4 Ownership of Capabilities to Test or Simulate

In the survey, there were specific questions about organisational capabilities to be useful in a test or simulation design. Overall, the respondents were positive about replicating organisations' IT/OT systems in a test environment. They also responded that they have ICT equipment to be used as a test laboratory. Also, 68% replied that they have resources to reproduce a possible attack.

Would you find it useful to replicate your organisation's IT / OT systems in a test environment so you can run test or simulate different scenarios? (optimalisation, vulnerability assessments, new purchases, implementations, etc).

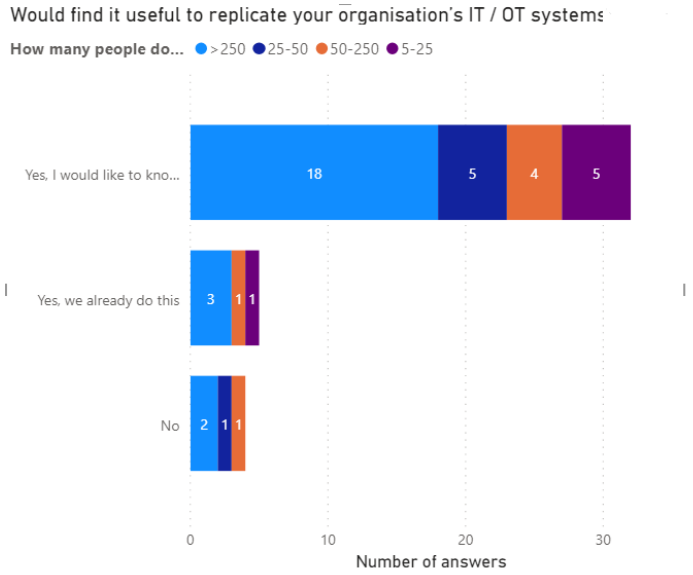

Figure 28 - Usefulness to replicate organisations systems to simulate scenarios

Do you have any ICT equipment that can be used as a test or simulation laboratory to test new approaches of your products or services?

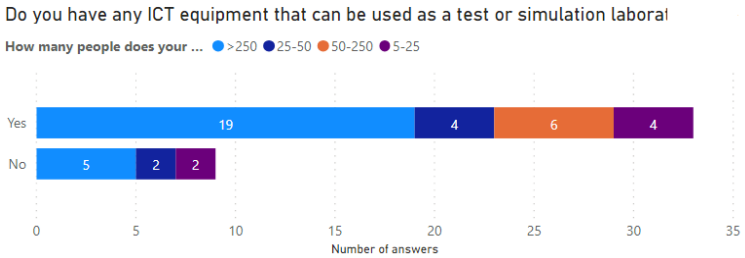

Figure 29 - Ownership of ICT equipment for a simulation

Do you have an ecosystem and supporting knowledgebase for evaluating IT products against new threats?

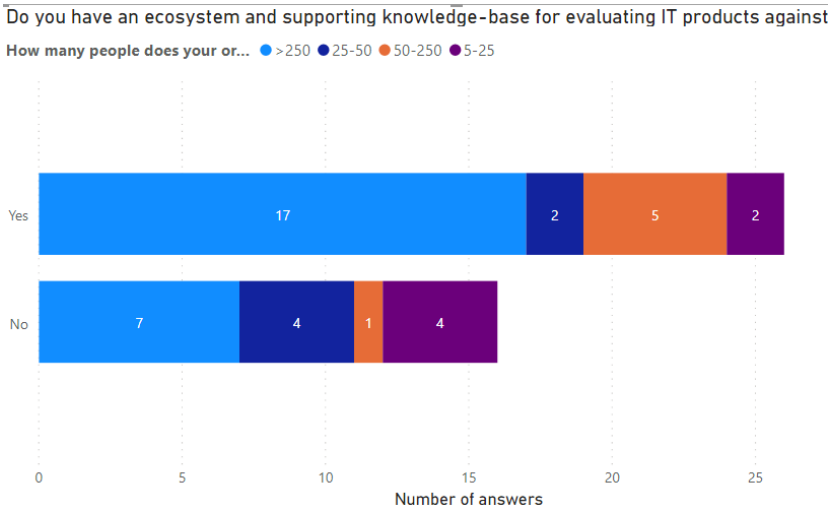

Figure 30 - Ownership of ecosystem of knowledge-base for evaluation

Do you have resources (personnel, skills and hardware) to reproduce a possible attack and prevent it from happening again?

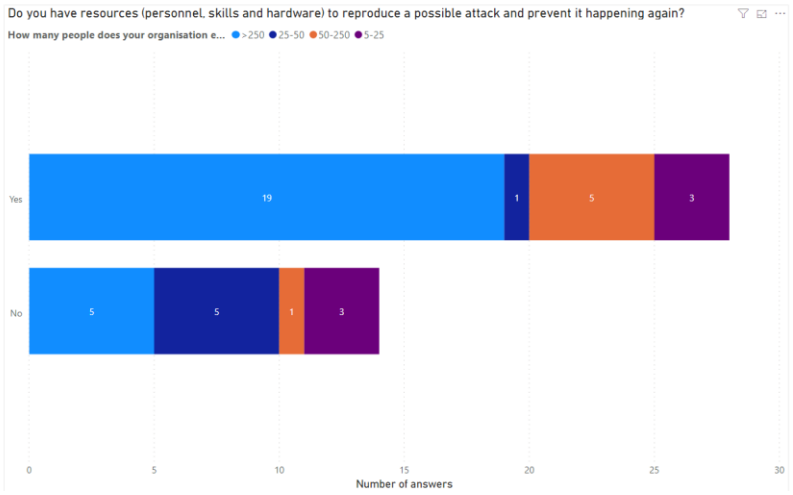

Figure 31 - Ownership of resources to reproduce a possible attack

2.4 Interest Towards a Cybersecurity Hub

The survey indicated that there is an interest to move towards a *European cybersecurity hub where providers can offer turnkey solutions customised to any kind of organisation*. 86% of the respondents replied that they would consider this kind of hub great. On the interest to use *a European cyber security marketplace where providers can offer cyber range services (training,*

testing, R&D, for example) customised to any kind of organisation and sector, the respondents indicated even more enthusiasm. 88% of the respondents would see this kind of hub as great.

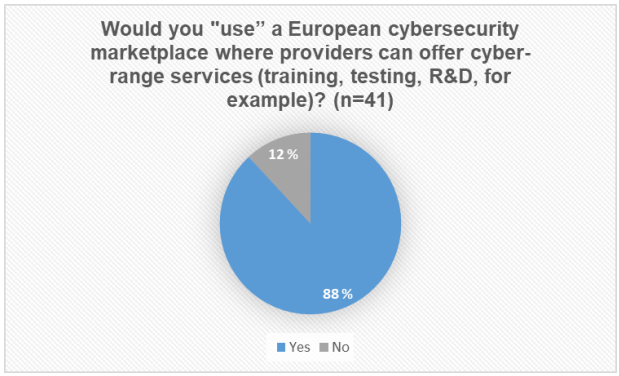

Figure 32 - Potential Use of a European Cybersecurity Marketplace

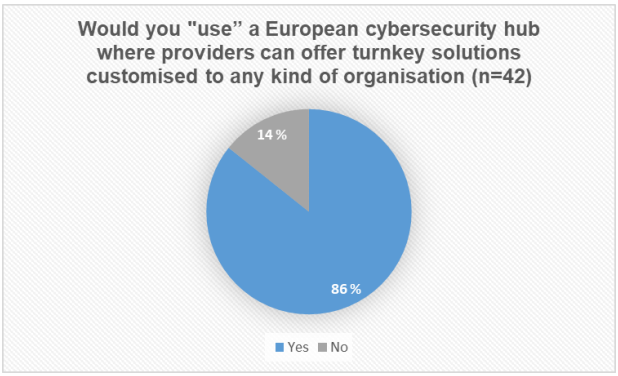

Figure 33 - Potential Use of a European Cybersecurity

3 Summary

Although there is a tremendous amount of product and process innovation occurring in the cybersecurity sector as digital paradigms continue to evolve, there is also much variability in the preparation for and mitigation of cyber risks, digital upskilling and capacity building, leaving organisations seeking “the right” solution. Cyber risk is also climbing ever higher on the list of priorities for a majority of the participating organisations. Nevertheless, establishing effective cybersecurity strategies remains challenging as many stakeholders still do not have enough information about the company’s cyber profile, level of resilience capability, or how to distribute resources for capacity building effectively. The need for a “European” applicable approach is clearly shown from results.

The respondents’ (n=43) backgrounds varied and they represented organisations with different sizes and from different European countries. The results give a picture about current practices around cybersecurity and the potential needs and requirements to provide services in the future and serve as a foundation for qualitative and quantitative analyses. Even the quick summary of the results show that respondents categorised cybersecurity as very important or important, but there are several gaps in the organisational capabilities, awareness and employees’ skills to implement cybersecurity issues in everyday life. Preparedness and mitigation towards cybersecurity threats can be seen as low, based on the responses of this survey. For example, only 39% of the respondents have financial vehicles (e.g. insurances) in case of cyber-attacks. Moreover, the organisations count on mitigation information for their self-assessments.

There seems to be consensus among respondents around the fact that security as an enabler is very important aspect and given clear frameworks to implement such measures and metrics would help to raise overall cyber resilience. The majority of the participants have a dedicated budget, yet the clear metrics of effectiveness is missing. The clear understanding of current level of cyber resilience and the potential fields of improvement and tools would give organisations the effective strategic plan to allocate their resources.

The European approach for simulation-based competence development is highlighted, for example in the form of cyber range services. The respondents were familiar with these definitions, provided specific needs of competence areas to be trained for the personnel, etc. The relevant cyber range service should be unique and designed for organisational purposes, with the use of the organisation’s own capabilities. However, these services should also be “plug‘n’play” solutions, offered as “off the shelf”, easy to set up and operate. These requirements are currently challenging to meet but they set the path for future cyber range and simulation-based competence development initiatives. Also, such services should be made affordable for smaller organisations as they are particularly keen on the highest return on their cybersecurity investments.

The different groups of participants have different skill needs, and as such, skills gaps differ per organisation. Also, the understanding of the missing skills differs, requiring different approaches for

participants to tackle them. Career paths are important, yet there is a demand for available tools and solutions for smaller organisations to implement it in their office culture and solutions. A European Cybersecurity Hub and an easy to use Cyber Range Marketplace is favored by the respondents as a potential trusted solution, connecting supply and demand and leveraging on the high quality of European soft skills available in the EU with a high demand for applicable cyber threat intelligence solutions.

Based on reactions to this report, the extended re-launch of the survey seems required to increase the pool of respondents and to further validate and / or iterate the current findings, as well as to create profiles of the different organisations and co-create turnkey solutions to raise the level of cyber resilience on a European level, especially in the current pandemic times.

ANNEX 1 Survey Questions

Your approach to cybersecurity

3.Do you consider cybersecurity important in your organisation?

- Very Important
- Important
- Neutral, like any other process
- Not very important
- Not at all

4.If it is important, how do you address it?

- We conduct regular vulnerability assesments by external providers
- We conduct regular inhouse vulnerability assesments
- We use security as an enabler (maintaining proper cyber hygiene and security measures positively affects business processes)
- We have dedicated in-house competence and capability building programmes
- We have out-sourced partners for handling cyber attacks

5.If cybersecurity is not yet important, what are the reasons for it?

- We do not know how to address it as it is complicated
- We do not have the money to dedicate to it
- We are not threatened by cyber attacks as we hardly operate in the cyber domain
- We are secure already and do not need to improve

6.Do you have dedicated budget for cybersecurity expenditure?

- Yes, it is more than 10% of our annual turnover
- Yes, it is less than 10% of our annual turnover
- No, but we plan to have it in a year time
- No, and we are not planning to have in the foreseeable future
-

7.When was the last time your organisation had a full scale vulnerability assessment?

- We have at least one annually
- Within a year
- More than a year
- Never had one
-

8.How do you know you are investing in the right tools and practices to raise cyber resilience?

- We conduct vulnerability assessments to identify potential points of failures
- We regularly have cyber exercises to define the level of corporate resilience and identify key milestones for improvement
- We have an external consultant guiding us and we rely on their expertise
- We know our needs based on our self-assessment and purchase products accordingly
- We make purchases not always understanding what we are actually purchasing
-

9.Do you have a dedicated in-house IT/cybersecurity team?

Yksi vaihtoehto

- Yes, we do
- No, we do not

10.Who is monitoring the IT/cybersecurity team and events?

Yksi vaihtoehto

- We have dedicated C-level IT security professionals for that (CISO, CIO, etc)
- They are reporting to the Head of IT
- They report directly to the MD/CEO
- They are a separate unit, and they do not have to report to anyone

11.Do you have any mandatory compliance requirements?

- Yes
- Not yet, but we will have soon
- No, and we will not need any soon

12.Do you have IT security compliance certification? (ISO, CC, CoBit, etc)

- Yes
- No

13.How do your inhouse business processes apply security concerns?

- During the planning process we cultivate the security/privacy by design principles
- We think of the business use cases and developments first and security second
- We are proactively engage in it (please specify how)
- We react to situations when they occur

14.How do you choose personnel to hire?

- We ask for MSc/BSc and certain industrial certifications (SANS, EC, etc) and if they qualify we hire them
- We check the educational background and the work experience. The latter is more important.
- We do not care about educational background, just about the work experience.
- We hire anyone who is willing to do the work and who has some form of basic understanding of the domain and then train him/her inhouse

15.Would you hire someone without a degree or higher level educational background, but with a proven competence?

- Yes, if the competence can be proven
- No, we cannot due to our inhouse policies

16.Are you familiar with the term: simulation based competence building?

- Yes
- I might have heard about it
- Doesn't ring a bell
- That is a type of construction work, right?

17.Do you know what a cyber-range is?

- Yes, we use it regularly
- Yes, we use it from time to time
- Yes, I know, but we don't use it
- No, but would like to know
- No, and I am happy with this

18.What are the key features you expect from a cyber-range service?

- [ ] Scalability
- [ ] Easy to setup
- [ ] Massive and robust computing power
- [ ] External accessibility
- [ ] Highly secure
- [ ] Federated with other ranges

- [ ] Plug and play contents for addressing special training needs
- [ ] Engaging content
- [ ] Should be able to host more than 100 participants
- [ ] Should allow the usage of own hardware and software
- [ ] Should provide all hardware and software solutions to conduct the exercise
- [ ] Should be automated

19.Would you prefer in-house or external training using a cyber-range?

Yksi vaihtoehto

- ○ In-house
- ○ External

20.Do you have cybersecurity related trainings available for your employees?

- ○ Yes, we do offer inhouse trainings for them
- ○ Yes, we offer external trainings for them
- ○ Yes, we have both inhouse and external trainings available to them
- ○ No, we don't invest in trainings, but are in the process to change this
- ○ No, we don't invest in trainings and this will not change soon
- ○

21.Is there a dedicated career path for employees?

- ○ Yes, we have an inhouse roadmap for them
- ○ No, but we support their career path progression by financing trainings and other activities
- ○ No, but we are planning to have
- ○ No, and we don't plan to have
- ○

22.How do you know which competences are missing from your organisation?

- [ ] We conduct assessments regularly to understand the various skillsets and focus on development based on that
- [ ] We ask our employees what they wish to learn and arrange trainings based on that

- [ ] We don't know, we guess
- [ ]

23.How do you measure competence building efficiency?

- We conduct assessments regularly to understand the various skillsets and focus on development based on that
- We conduct regular cyber exercises and learn from the results
- We see if the business is growing or not
- We don't
-

24.How do you measure cost effectiveness of cybersecurity expenditures?

- We have historical data mapped against potential cyber threats and make decisions based on the analyses
- We have a fixed budget to spend each year, regardless of what the threats are
- We didn't think so far it should be measured
- We don't
-

25.Would you purchase cybersecurity services from a European provider but from another country?

- Yes, of course, if they have a proven track record
- Yes, we do it all the time
- Yes, but we have done it rarely
- We haven't so far but we are not against it
- No, we support local markets and providers
- No, we are obliged to use local providers
-

26.How much of your turnover do you or would you allocate to cybersecurity training for your staff?

Yksi vaihtoehto

- More than 20 %
- Less than 20%

- 0%

27.Do you favour European solutions over non-European ones?

- Yes, in case there is an equally good solution to our issue we choose the European provider
- Yes, it is our corporate policy
- No, we only care about the benefits regardless of the country of origin
- Never thought of it before

28.How do you handle supplier chain risk?

- We mitigate supplier risk our contractual terms, the responsibilities and technical assessments are mandatory before we connect with them digitally (eg data exchange, server access, etc)
- We have an insurance coverage
- We cannot deal with the issue because of our position in the supply chain
- We don't

29.Do you have financial vehicles to mitigate potential cybersecurity risks?

- Yes, we use cyber insurance to cover certain types of incidents
- No, we don't but we are looking into it already
- No, and we don't plan to as it is expensive
- No, and we don't plan to as we don't know what it is
- No, we don't plan to as we are good without it

30.Would you "use" a European cybersecurity hub where providers can offer turnkey solutions customised to any kind of organisation?

- Yes, it sounds just great
- I don't know as it is still too complicated for us
- No, we stick to our current channels

31.Would you "use" a European cybersecurity marketplace where providers can offer cyber-range services (training, testing, R&D, for example) customised to any kind of organisation and sector?

- Yes, it sounds just great
- I don't know as it is still too complicated for us
- No, we stick to our current channels

32.What type of organisation are you?

- Public
- Private

33.How many people does your organisation employ?

- 0-5
- 5-25
- 25-50
- 50-250
- >250

34.What do you think is mainly missing from your organisation to raise the level of cyber resilience? You can list anything that comes into your mind

35.What are the key cybersecurity skills that you demand from your employees?

- [ ] Situational awareness
- [ ] Communication
- [ ] Leadership
- [ ] Collaborative and approachable
- [ ] Writing ability
- [ ] Deep technical understanding of all aspects of IT domain
- [ ] Programming
- [ ] Understanding cloud security
- [ ] Analytic mindset

- [ ] Hacker mindset
- [ ] Understanding architecture, administration and operating systems
- [ ] Database knowledge

36.Who should be trained using a cyber-range in your organization?

- ○ All of them
- ○ Only IT staff
- ○ Only non-IT staff
- ○ Only Management
- ○ All of them, subcontractors and service providers included
- ○

37.What are the acceptable costs of cyber related training (in % of cybersecurity budget)?

- ○ 0-10
- ○ 10-20
- ○ 20-30
- ○ 30-40
- ○ 40-50
- ○ 50-60
- ○ 60-70
- ○ 70-80
- ○ 80-90
- ○ 90-100

38.Would find it useful to replicate your organisation's IT / OT systems in a test environment so you can run test or simulate different scenarios? (optimalisation, vulnerability assessments, new purchases, implementations, etc).

- ○ Yes, I would like to know more about it
- ○ Yes, we already do this
- ○ No

39.Do you have any ICT equipment that can be used as a test or simulation laboratory to test new approaches of your products or services?

- Yes
- (●) No

40.Do you have an ecosystem and supporting knowledge-base for evaluating IT products against new threats?

- Yes
- No

41.Do you have resources (personnel, skills and hardware) to reproduce a possible attack and prevent it happening again?

- Yes
- No

ANNEX 2 Correlation

There is a correlation between questions "*Do you consider cybersecurity important in your organization*?" and "How do you know you are investing in the right tools and practices to raise cyber resilience?" (Correlation 0,336 sig 5 % level) and "How do you choose personnel to hire" (Correlation 0,399, sig 5 % level) and "How do you measure cost effectiveness of cybersecurity expenditures?" (correlation 0,593 sig 1 % level) and "Do you have an ecosystem and supporting knowledge-base from evaluating IT products against new threats?" (Correlation 0,348 sig 5 % level)

Also question "*If it is important (cybersecurity), how do you address it*?" correlate with question "How do you handle supplier chain risk?" (Correlation 0,371 sig. 5 % level).

Question "*Do you have dedicated budget for cybersecurity expenditure?"* correlate with "How much of turnover do you or would you allocate to cybersecurity training for your staff?" (Correlation 0,482 sig. 1 % level) and "Do you have financial vehicles to mitigate potential cybersecurity risks?" (Correlation 0,423 sig. 5 % level).

Question "*When was the last time your organization had a full scale vulnerability assessment?"* correlate with question "How do you know you are investing in the right tools and practices to raise cyber resilience?" (Correlation 0,413 sig. 1 % level), and "Do you have a dedicated in-house IT/cybersecurity team?" (Correlation 0,416 sig. 1 % level) and "Mandatory compliance requirements?" (Correlation 0,341 sig. 5% level) and "How do you choose personnel to hire?" (Correlation 0,356 sig 5 % level)

Question "*How do you know you are investing in the right tools and practices to raise cyber resilience*?" correlate with question "Do you consider cybersecurity important in your organization?" (Correlation 0,336 sig. 5% level) and "When was the last time your organization had a full scale vulnerability assessment?" (Correlation 0,413 sig. 1 % level) and "Do you have dedicated in-house IT/cybersecurity team?" (Correlation 0,416 sig 1 % level) and "Are you familiar with the term: simulation based competence building?" (Correlation 0,314 sig 5 % level).

Question "*Do you have a dedicated in-house IT/cybersecurity team?"* correlate with question "When was the last time your organization had a full scale vulnerability assessment?" (Correlation 0,416 sig 1 % level), and "Do you have IT security compliance certification (ISO, CC, CoBit, etc)? (Correlation 0,431 sig 1 % level), and "Would you prefer in-house or external training using a cyber-range?" (Correlation 0,323 sig. 5 % level) and "Do you favor European solutions over non-European ones?" (Correlation 0,436 sig 1 % level), and "Do you have an ecosystem and supporting knowledge-base for evaluating IT products against new threats?" (Correlation 0,310 sig. 5 % level) and "Do you have resources (personnel, skills and hardware) to reproduce a possible attack and prevent it happening again?" (Correlation 0,372 sig. 5 % level)

Question "*Who is monitoring the IT/cybersecurity team and events*?" correlate with question "Do you have IT security compliance certification (ISO, CC, CoBit, etc.)?" (Correlation 0,413 sig 1 % level).

Question "*Do you have any mandatory compliance requirements*?" correlate with question "When was the last time your organization had a full scale vulnerability assessment?" (Correlation 0,341 sig. 5 % level), and "What type of organization are you?" (Correlation 0,332 sig. 5 % level).

Question "*Do you have IT security compliance certification (ISO, CC, CoBit etc?"* correlate with question "Do you have a dedicated in-house IT/cybersecurity team?" (Correlation 0,431 sig. 1 % level) and "Who is monitoring the IT/cybersecurity team and events?" (Correlation 0,413 sig 5 % level), and "Do you favor European solutions over non-European ones?" (Correlation 0,326 sig. 5 % level), and "How many people does your organization employ?" (Correlation -0,388 sig. 5 % level).

Question "*How do your inhouse business processes apply security concerns*?" correlate with questions "Would you use a European cybersecurity marketplace where providers can offer cyber-range services (Training, testing, R&D, for example) customized to any kind of organization and sector?" (Correlation 0,383 sig. 5 % level).

Question "*How do you choose personnel to hire?"* correlate with question "Do you consider cybersecurity important in your organization?" (Corelation 0,336 sig 5 % level), and "Do you have dedicated budget for cybersecurity expenditure?" (Correlation 0,356 sig 5 % level).

Question "*would you hire someone without a degree or higher level educational background, but with a proven competence?"* did not correlate with any question.

Question "*Are you familiar with term: simulation based competence building*?" correlate with question "Do you consider cybersecurity important in your organization?" (Correlation 0,399 sig 1 % level), and "When was the last time your organization had a full scale vulnerability assessment?" (Correlation 0,314 sig 5 % level), and "How do you measure competence building efficiency?" (Correlation -0,381 sig. 5 % level), and "Do you favor European solutions over non-European ones?" (Correlation 0,319 sig 5 % level), and "Would you use European cybersecurity marketplace where providers can offer cyber-range services (Training, testing, R&D, for example) customized to any kind of organization and sector?" (Correlation 0,471 sig 1 % level).

Question *"Do you know what a cyber-Range is*?" did not correlate with any other question.

Question "*Would you prefer in-house or external training using a cyber-range*?" correlate with question "Do you have a dedicated in-house IT/cybersecurity team?" *(Correlation 0,323 sig 5 % level), and "How do you measure competence building efficiency?" (Correlation 0,414 sig 1 % level), and "Do you have resources (personnel, skills and hardware) to reproduce a possible attack and prevent it happening again?" (Correlation 0,352 sig, 5 % level).

Question "*Do you have cybersecurity related trainings available for your employees*?" correlate with question "Is there a dedicated career path for employees?" (Correlation 0,315 sig 5 % level), and "How do you handle supplier chain risk? " (Correlation 0,424 sig 1 % level).

Question "*Is there a dedicated career path for employees*?" correlate with question " Do you have cybersecurity related trainings available for your employees?"(Correlation 0,315 sig. 5 % level) , and " How do you measure cost effectiveness of cybersecurity expenditures?" (correlation 0,407 sig 1 % level)

Question "*How to know which competences are missing from your organization*?" did not correlate with any question.

Question "*How do you measure competence building efficiency*?" correlate with question "Are you familiar with the term: simulation based competence building?" (Correlation -0,381, sig. 5 % level), and "Would you prefer in-house or external training using a cyber-range?" (Correlation 0,414 sig 1 % level), and " Is there a dedicated career path for employees" (correlation 0,407 sig. 1 % level), and "Do you have financial vehicles to mitigate potential cybersecurity risks?"(Correlation 0,388 sig 5 % level), and "How many people does your organization employ?" (Correlation -0,324 sig 5 % level), and "Do you have any ICT equipment that can be used as a test or simulation laboratory to test new approaches of your products or services?" (Correlation -0,414 sig 1 % level).

Question "*How do you measure cost effectiveness of cybersecurity expenditures*?" correlate with question "Do you consider cybersecurity important in your organization?" (Correlation 0,593 sig. 1 % level), and "Would you use a European cybersecurity hub where providers can offer turnkey solutions customized to any kind of organization? " (Correlation 0,563 sig. 1 % level) and, "Would you use a European cybersecurity marketplace where providers can offer cyber-range services (training, testing, R&D, for example) cutomised to any kind of organization and sector? " (Correlation 0,867 sig. 1 % level).

Question "*Would you purchase cybersecurity services from a European provider but from another country?"* did not correlate with any question "

Question *"How much of your turnover do you or would you allocate to cybersecurity training for your staff?"* correlate with question "If cybersecurity is not yet important, what are the reasons for tit?" (Correlation 0,482 sig 1 % level), and "Do you have financial vehicles to mitigate potential cybersecurity risks? " (Correlation 0,371 sig. 5 % level).

Question "*Do you favour European solutions over non-European ones?"* correlate with question "Do you have a dedicated in-house IT/cybersecurity team?" (Correlation 0,436 sig. 1 % level), and "Do you have IT security compliance certification (ISO, CC, CoBit, etc)?" (Correlation 0,326 sig 5 % level) and "Are you familiar with the term: simulation based competence building?" (Correlation 0,319 sig 5 % level), and "Do you have any ICT equipment that can be used as a test or simulation laboratory to test new approaches of your products or services?" (Correlation 0,398 sig. 5 % level).

Question "*How do you handle supplier chain risk*?" correlate with question "If it si important, how do you address it?" (Correlation 0,371 sig. 5 % level), and "Do you have cybersecurity related trainings available for your employees?" (Correlation 0,424 sig. 1 % level), and "Do you have financial vehicles to mitigate potential cybersecurity risks?"(Correlation 0,560 sig 1 % level).

Question "*Do you have financial vehicles to mitigate potential cybersecurity risks?"* correlate with question "I cybersecurity is not yet important, what are the reasons for it?" (Correlation 0,423 sig. 1 % level), and "How do you measure competence building efficiency? " (0,388, sig. 5 % level), and "How much of your turnover do you or would you allocate to cybersecurity training for your staff? " (Correlation 0,371 sig. 5 % level), and "How do you handle supplier chain risk? " (Correlation 0,560 sig. 1 % level).

Question "*Would you use a European cybersecurity hub where providers can offer turnkey solutions customized to any kind of organization?"* correlate with question "How do you measure cost effectiveness of cybersecurity expenditures?" (Correlation 0,563 sig. 1 % level), and "Would you use a European cybersecurity marketplace where providers can offer cyber-range services (training, testin, R&D, for example) customized to any kind of organization and sector?"(Correlation 0,697 sig 1 % level), and "What type of organization are you?" (Correlation -0,420 sig 5 % level).

Question "*Would you use a European cybersecurity marketplace where providers can offer cyber-range services (training, testing, R&D, for example) customized to any kind of organization and sector?"* correlate with question "How do your inhouse business processes apply security concerns?" (Correlation 0,383 sig. 5 % level), and "Are you familiar with the term: simulation based competence building? " (Correlation 0,471 sig 1 % level).

Question "*What type of organization are you?"* correlate with question "Do you have any mandatory compliance requirements?" (Correlation 0,332 sig. 5 % level), and "Would you use a European cybersecurity hub where providers can offer turnkey solutions customized to any kind of organisations? " (Correlation -0,420 sig. level 1 %), and "How many people does your organization employ? " (Correlation -0,374 sig 5 % level), and "Do you have resources (personnel, skills and hardware) to reproduce a possible attack and prevent it happening again?" (Correlation 0,308 sig. 5 % level).

Question "*How many people does your organization employ*?" correlate with question "Do you have IT security compliance certification (ISO, CC CoBit, etc)?" (Correlation -0, 388 sig. 5 % level), and " How do you measure competence building efficiency?" (Correlation -0,324 sig. 5 % level), and "Do you have resources (personnel, skills and hardware) to reproduce a possible attack and prevent it happening again?" (Correlation -0, 374 sig. 5 % level).

Question "*Who should be trained using a cyber-range in your organization?* " correlate with question "Would find it useful to replicate your organisation's IT/OT systems in a test environment so you can run test or simulate different scenarios? (Optimization, vulnerability assessments, new purchases, implementations, etc)?" (Correlation 0,417 sig. 5 % level), and "Do you have any ITC equipment that can be used as a test or simulation laboratory to test new approaches of your products or services? " (Correlation 0,427 sig. 1 % level) , and "Do you have an ecosystem and supporting knowledge-base for evaluating IT products against new threats? " (Correlation 0,427 sig. 1 % level).

Question *" What are the acceptable costs of cyber related training (in % of cybersecurity budget)?"* correlate with no other question.

Question "*Would find it useful to replicate your organisation's IT/OT systems in a test environment so you can run test or simulate different scenarios? (Optimalisation, vulnerability assessments, new purchases, implementations, etc)?"* correlate with question "Who should be trained using a cyber-range in your organization?" (Correlation 0,417 sig 5 % level).

Question "*Do you have any ICT equipment that can be used as a test or simulation laboratory to test new approaches of your products or services?"* correlate with question "Who should be trained using a cuber-range in your organization? " (Correlation 0,427 sig. 1 % level) .

Question *"Do you have ecosystem and supporting knowledge-base for evaluating IT products against new threats?"* correlate with question " Do you consider cybersecurity important in your organization?" (Correlation 0,348 sig. 5 % level), and "Do you have a dedicated in-house IT/cybersecurity team?" (Correlation 0,310, sig. 5 % level) and " Who should be trained using a cyber-range in your organization?" (Correlation 0,427 sig. 1 % level), and " Do you have resources (personnel, skills and hardware) to reproduce a possible attack and prevent it happening again?" (Correlation 0,693 sig. 1 % level).

Question "*Do you have resources (personnel, skills and hardware) to reproduce a possible attack and prevent it happening again?* " correlate with question "Do you have a dedicated in-house IT/Cybersecurity team?" (Correlation 0,372 sig. 5 % level), and " Would you prefer in-house or external training using a cyber-range?" (Correlation 0,352 sig. 5 % level), and "What type of organization are you? " (Correlation 0,306 sig 5 % level) , and "How many people does your organisation employ? " (Correlation -0,374 sig 5 % level) and. "Do you have an ecosystem and supporting knowledge-base for evaluating IT products against new threats?" (Correlation 0,693 sig. 1 % level)