CYBERNETICA

Cybersecurity Domain Analysis

Public

Document ID: D-2-391
Version: 1.02
Date: 14.02.2022

Cybernetica research reports are available online at https://research.cyber.ee.

Mailing address:
Cybernetica AS
Mäealuse 2/1
12618 Tallinn
Estonia

Table of Contents

1. The Summary

The paper analyzes characteristic properties of the emerging cybersecurity market from the perspective of a company planning to enter that market. Cybersecurity is not limited to pure technical knowledge but makes an extensive use of many systemic disciplines. It deals with processes and organization, risks, training, management, team building and even psychology. This way, the extent of the cybersecurity market is substantially wider than technical solutions only. The appeal of tackling the major segments of the cybersecurity market is analyzed, tabulated and illustrated.

The research derives from an internal evaluation of cybermarket proceeded by Cybernetica AS.

2. Introduction

Cybersecurity as a discipline is the result of globally applying the information technology on the society. While information security as a discipline dealt mostly with the local (or sometimes global) protection of secrets, cyber security is responsible for keeping a global computerized society resilient. This includes protecting information from faults and errors, securing computers from human agents, securing the population from computers with bad reputation. Most importantly, this includes protecting a whole class of information systems the society is dependent (e.g. for governance purposes) from any hazard or malicious agent. Obviously, the security of such a complex interdependence does not come as granted but has to be meticulously maintained. The higher is the criticality of a managed homeostasis, the more dangerous are seen the threats around it and attacks against it. This is why commercially offered protections (solutions, technologies and techniques) are widely used to maintain the cybersecurity balance and how they form the cyber security market.

The global cybersecurity market size was estimated to be USD 162.5 billion in 2020 and is projected to register a CAGR of 12.5% to reach USD 418.3 billion by 2028. Security solutions have been gaining momentum worldwide as the incidence of cyber-attacks has increased at an unprecedented pace.

In today's evolving digital world, defences against the online threats are becoming increasingly important. There is a need to fight the organised cybercrime, rising incidence of fraud and technical vulnerabilities.

Cybersecurity domain is growing quickly and is in constant change. There are new ways to cope with ever changing environment, threats, technologies and opportunities.

Thus, it is important for any company active in the domain to create and maintain a plan about it, how will the company change and develop its business models to achieve a sustained value creation. Companies that are willing to create value over an extended period of time, have to successfully adapt and renew their business models.

Business in the continuously growing domain should be planned with an orientation

towards experimenting with and exploiting new business opportunities; a balanced use of resources; as well as achieving coherence between leadership, culture, and employee commitment - these actions together will shape the key strategising actions.

In this document the sub-domains of the cybersecurity are explored regarding the perspective of the entry barriers. Hopefully this document will assist an organisation while planning to enter the cybersecurity market. It also will assess the attractiveness of various sub-domains of cybersecurity and help to understand the barriers hindering the successfully entry to cyber markets.

3. Cybersecurity domain

Figure 1 Cybersecurity Domain presents a mindmap of the whole cybersecurity domain with various branches color-coded and related key-words listed.

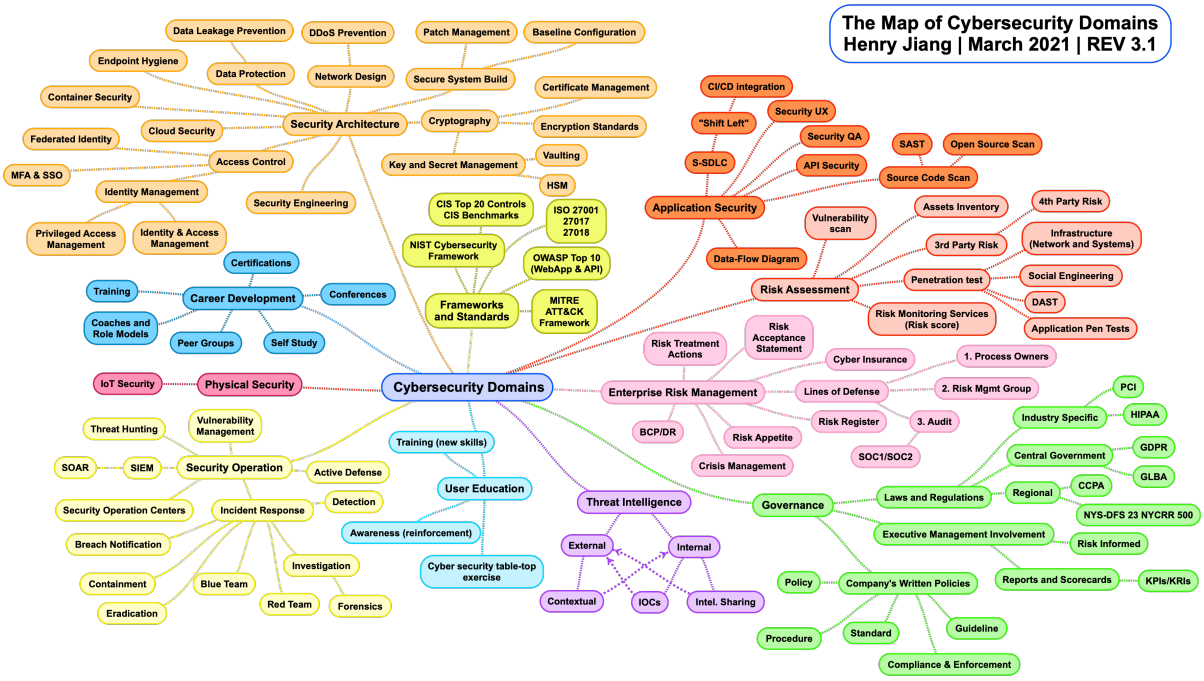

Figure 1. Cybersecurity Domain

Throughout the rest of the document, these branches of cybersecurity domain are taken and evaluated based on the following attributes:

- Scalability,
- Brand enhancing,
- Business-enabling (open the doors),
- High start-up costs,
- Strong (known) brands exist on the market,
- There exists an established competition with substantial resources to retaliate,
- High spending on advertising by incumbents,

- Licenses or regulatory clearance required,
- High switching costs, high customer loyalty,
- There exist proprietary product technologies,
- Steep learning or experience curve,
- Cultural sensitivity,
- Strong trust of individuals and company needed,
- Favorable geographical locations (important to be present there).

The original aim of the research was to evaluate the subdomains (branches) of cybersecurity from the perspective of the attributes ensuring a quick entrance to the cybersecurity market. The attributes contributing to that were: low customer loyalty, low learning curve, low start-up cost, business enabling etc. It is worth to notice these branches will (although not always) have somewhat opposite attributes compared to the strategic branches companies would like to participate in the long run. Strategic branches obviously have higher start-up cost, high customer loyalty, a steeper learning curve, a potential to scale up the business etc.

Then each branch of the cybersecurity domain was scored on the scale from 1 to 5 (5 being very favourable and 1 not favourable at all). Two prospects are presented in this research:

- Tactical score represents an instant interest, denoting a short term goal for participation in the cybersecurity domain.
- Strategic score represents a long term interest, denoting the perspectives the cybersecurity company would like to reach in the long run.

In case of a high tactical score, the subdomains are to be explored in a more detailed way.

4. Subdomain analysis

Throughout the rest of the document, sub-domains (branches) of the cybersecurity field are analysed according the criteria (attributes) listed in previous chapter. The subdomains correspond to the differently coloured areas on Figure 1 Cybersecurity Domain.

4.1. Frameworks and standards

The frameworks and standards domain addresses creation and maintenance of all forms of cybersecurity standards and frameworks. In addition, it deals with standard vocabulary, defining concepts, professional competencies, and standard best practices.

Most of the framework and standards domain is lead by well recognised and long established international, often non-profit, organisations where a lot of work is based on

voluntary base.

Assessment

To enter the market it requires remarkable start-up costs, there are strong (known) brands already on the market, most of them are of academic or public background and non-profit organisations. There are opportunities for offering tools that help the implementation of frameworks and standards.

- **Tactical interest score:** 1/5
- **Strategical interest score:** 2/5

4.2. Application security

Application security is about management of the security lifecycle of in-house developed, hosted, or acquired software. The main target is to prevent, detect, and remediate security weaknesses before they will impact the enterprise.

Today's applications are developed, operated and maintained in a highly complex, diverse, and dynamic environment. Applications run on multiple platforms: web, mobile, cloud, etc., and may be based on application architectures that are much more complex than legacy structures of client-server or database-web type. Development lifecycles have become shorter; transitioning became from months or years in long waterfall methodologies, to DevOps cycles with frequent code updates. Also, applications are rarely created from scratch, and are often "assembled" from a complex mix of development frameworks, libraries, legacy code and new code.

Application vulnerabilities exist for many reasons: insecure design, insecure infrastructure, coding mistakes, weak authentication, and failure to test for unusual or unexpected conditions. Different techniques are used to surface such security vulnerabilities at different stages of an application's lifecycle, such as design, development, deployment, upgrade, maintenance.

Secure building of applications is an internal concern of all development teams, but the domain offers service opportunities which help to build the governance and management by providing tools to support the secure software development lifecycle. Examples of such tools are: continuous integration/delivery solutions, automatic source code scanning etc. Additionally, the management may wish to apply a third party assessment to their in-house built software or for procured components. One may order a software design review, source code review or source code scanning as a service.

Assessment

Application security is a domain with steep learning and experience curves. The organisation entering the market should most-likely be previously involved in development of cybersecurity critical applications. The domain is offering service and product opportunities mostly for application developers.

Strategically there exist a field of application security certification (eg. TÜV - Technischer Überwachungsverein) with a very high entry cost and customer loyalty.

- **Tactical interest score:** 3/5
- **Strategical interest score:** 3/5

4.3. Risk assessment

Risk assessment helps to identify and categorise risks and provides an outline for potential consequences. Performing a risk assessment involves processes and technologies that help identify, evaluate and report on any risk-related concern. It should be mentioned that risk-centered approaches are characteristic primarily to developed nations.

Risk assessment is a “key component” of the risk management process and is primarily focused on the identification and analysis phases of risk management. It involves

- identification of the critical assets and sensitive data,
- building a risk profile for each asset,
- determination of cybersecurity risks for each asset,
- mapping of links of critical assets,
- asset prioritisation.

There are some additional to assessment steps which rather belong to risk treatment and quality loop and further elaborate the risk assessment, like:

- risk treatment, e.g. creation of mitigation plan with security controls to eliminate or mitigate the impact of each risk,
- continually monitoring of risks, threats, and vulnerabilities.

Risk assessment in this context is a function of cybersecurity, where an organisation evaluates its most important IT assets and their vulnerabilities. IT risk assessment is not directed to organisation’s macro level operations which are subject to Enterprise risk management domain.

Assessment

Risk assessment is a field which is clearly understood by a large number of organisations. The concern of being hacked, watched, attacked or systems been compromised is there and recent news and media attention is feeding the fear which gives a lot of opportunities in the field. Ethical hacking and scanning for vulnerabilities is something that a lot of young people find fascinating, still it requires certain skills and experience and has a remarkable learning curve. The domain is further business-enabling, meaning that risk assessment is continuous in its nature and needs to be conducted regularly. Additionally, by identifying the vulnerabilities, the organisation can propose measures to

protect against the threats and can also offer the services from Application security and Security architecture subdomains. It also will open opportunities in the User education field where trainings and couching of various levels can be offered. This domain probably is of immediate interest for any neophyte and a good entry point to the field of cybersecurity.

- **Tactical interest score:** 5/5
- **Strategical interest score:** 4/5

4.4. Enterprise risk management

Enterprise risk management involves the identification, vocabulary analysis, evaluation, and prioritisation of current and potential risks. This allows one to address loss exposures, to monitor risk control and financial resources in order to minimise possible adverse effects of potential loss. Further, a solid risk management strategy gives an organisation the ability to maximise the realisation of available opportunities while avoiding risks.

Risk management is a management discipline that evaluates which risks to take into the scope of Risk assessment. Unlike risk assessment, risk management is an umbrella term that includes risk assessment as one of the key stages. Risk management can never be completed 100% in one attempt. It is a continuous process where an organisation keeps monitoring the existing risks and listing new risks as they evolve or are identified.

Assessment

Cybersecurity risk management requires an in-depth knowledge of your particular business, and consideration of factors ranging from the industry and company size to organisations' business model and practices. It's one of those areas and organisation is willing to be hands-on rather than completely turning it over to a third party.

If an organisation cannot have a full-time, in-house chief information security officer (CISO), it may be a better option to hire a consultant rather to outsource the entire strategic function. Many security companies and professionals also offer virtual CISO (often called vCISO) services, which help to build a consistent relationship with an expert who gets to know the needs and business of the organisations.

Still, such a consulting business does not scale well. It is of a domestic nature and has a steep learning curve pertaining a specific organisation. Thus, the opportunities related to the domain are rather related to the Career development domain, under which various coaching, CISO trainings and audits can be offered.

Most interesting opportunity for this the domain is related to risk management products, e.g. tools providing somewhat systematic documentation and support to risk management processes assisting CISOs with a systematic approach to risk management activities. It may be e.g. tools that join Governance and Risk assessment into one logical process, to consolidate the IT asset inventory, risk quantification solution, incident

management etc. into one information system.

- **Tactical interest score:** 3/5
- **Strategical interest score:** 4/5

4.5. Governance

In cybersecurity, governance is the system by which an organisation directs and controls IT security. Governance determines who is authorised to make decisions. It also specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated. Governance does not ensure that controls are implemented to mitigate risks which is a concern of Enterprise risk management. Governance ensures that security strategies are aligned with business objectives and consistent with regulations.

This is the domain that doesn't "get your hands dirty with the technical stuff". It's basically like the government which sets and controls laws, administration, auditing, etc. However, few of these subdomains do require prior experience in information security and some minimum knowledge in this domain. This is the place where people with no prior IT experience can also enter. Governance mainly comprises of auditing, laws, policies and procedures, compliances, etc. All the standards and checklists stuff come under this. The people working in this are responsible to check if their organisation and its employees are following and maintaining all the industry standards set by well-known Frameworks and standards organisations such as ISO, OWASP, etc.

Assessment

Due to the non-technical nature of the domain it attracts many service providers that are active in the field of business consultancy and advisory. Although the domain can be considered to be a shortcut to executive management and might be business-enabling to more technical services, it may not be the best initial priority for an organisation interested in cybersecurity market.

Governance may be supported by technical tools already described in the Assessment paragraph of the Enterprise risk management chapter.

- **Tactical interest score:** 3/5
- **Strategical interest score:** 4/5

4.6. Threat intelligence

Threat intelligence is data that is collected, processed, and analysed to understand a threat actor's motives, targets, and attack behaviours. Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets.

Threat intelligence enables organisations to make faster, better reasoned, data-backed security decisions and extend their behaviour in the fight against the threat actors from reactive to proactive. Threat intelligence:

- sheds light on the unknown, enabling security teams to make better decisions;
- empowers cyber security stakeholders by revealing adversarial motives and their tactics, techniques, and procedures (TTPs);
- helps security professionals better understand the threat actor's decision-making process;
- empowers business stakeholders, such as executive boards, CISOs, CIOs and CTOs; to invest wisely, better mitigate risks, become more efficient and make faster decisions.

For most organisations gathering, qualifying and organising this type of information on their own would be too costly. This is why they need a trusted partner who can provide qualified and actionable Threat Intelligence data that can be used to take both operational and strategic decisions.

Assessment

The people working in this domain are cyber threat analysts and to become one you need to have immense knowledge of information security as well as the knowledge in networking. Despite the fact that threat intelligence benefits organisations of all shapes and sizes, it assumes a dedicated IT security analyst, SOC, CSIRT, or intel analyst to be present in the organisation.

Surely, a systematic gathering of threat information should be a part of every organisation providing cybersecurity services. Organisation should start gathering threat intelligence data systematically to educate itself and with the potential of being a threat intelligence service provider later. It is important to have up-to-date information about motives of the adversaries as well as on their tactics, techniques, and procedures.

In case a sufficient database and experience available, it is possible to start selling the information or providing awareness reinforcement trainings (see more in User education). Risk management products, too, should have a threat intelligence feed to help users to mitigate current risks.

- **Tactical interest score:** 1/5
- **Strategical interest score:** 5/5

4.7. User education

Cybersecurity user education is the process of facilitating learning, or the acquisition of knowledge, skills, values, morals, beliefs, and habits of information technology users and raising the awareness of how to protect oneself and the organisation in cyberspace. Educational methods include teaching, training, storytelling, discussion as well as

certification of users.

Users can be a company's weakest link — or its first line of defence. How well users play this role depends on organisation's willingness to invest in security awareness training, as well as their ability to support that training through the institutional technologies and processes.

To deliver an effective protection for the network and applications, the organisation should educate the users and engage them through exercises. There can be classical awareness trainings, cyber security training courses to provide the employees with the most current information about attack vectors, or more complex simulated attacks — for example, sending out fake phishing emails to help employees learn how to recognise threats.

Additionally, there can be combined approaches where integrated platforms offer hours of security awareness training content, phishing templates, and results reporting — all in one place.

Assessment

Nowadays the traditional classroom trainings have been replaced with on-line trainings and that provides the scalability of opportunities. Also, training large groups of people is business-enabling.

- **Tactical interest score:** 4/5
- **Strategical interest score:** 4/5

4.8. Security operations

Security operations are concerned with the day-to-day access of system resources as well as with their security. This means that there must be a Security Operations Center (SOC) framework in place consisting of the proper policies, standards, procedures and guidelines for the core and support services of an organisation.

The SOC is a centralised function within an organisation employing people, processes, and technology to continuously monitor and improve the security posture of the organisation while preventing, detecting and analysing cybersecurity incidents, and responding to these.

When a SOC is developed in-house, the challenges include lack of skilled resources, an expensive technology stack and lack of the reporting metrics. There are possibilities to outsource the managed security which helps address these challenges. It is considered that SOC-as-a-Service (SOCaaS) costs 80% less than building your own. However, SOCaaS does not replace the function entirely, thus the internal willingness to contribute to the security operations must remain at place.

While it is unavoidable for micro and small businesses to need SOCaaS to fulfil all the

SOC functions, the large enterprises tend to use SOCaaS analyst teams to supplement their internal teams, while medium-sized organisations typically fall somewhere in between these extremes.

As a result, most SOCaaS providers are typically specialising to focus on one or two of these sub-segments, with very few catering equally to all market segments. The trend of specialising to serve the needs of a particular market sub-segment is expected to continue.

SOCaaS suppliers focusing on SMEs will hone offerings to provide insights and guidance to enable organisations to co-manage their security with external SOC teams, for example, while suppliers focusing on medium, large and very large enterprises will expand their capabilities around risk, edge security, and Operational Technology and IoT security.

Assessment

To become a part of the Security Operations domain there are two options: to provide SOC-As-A-Service or to provide specific tools and services for SOCs.

SOCaaS requires threat intelligence of an excellent quality, around-the-clock teams available to quickly analyse and respond to alerts, and state-of-the-art tools to detect incidents.

SOCaaS has a very steep learning and experience curve. Providing SOCaaS requires high start-up costs. Most likely the customer loyalty is high in the field because changing the provider or tools in this area is expensive - resulting high switching costs for a customer. In addition to that the local presence and a direct contact with the customers is assumed.

Another option is to provide specific tools and services to enable SOCs. these may be related to threat intelligence feeds, incident detection, management and monitoring tools (SIEM) and recovery solutions.

Despite a product option is more scalable, the provision of a service seems to remain more stable and sustainable in a constantly changing market environment and thus strategically more appealing as provides a stable revenue for a longer period.

This domain can be very hard to get into, while strategically very appealing.

- **Tactical interest score:** 2/5
- **Strategical interest score:** 5/5

4.9. Physical security

Physical security refers to all the controls that should be applied to the physical hardware within organisations purview.

Physical security asks the following questions:

- Is there a fencing around the facility that forces individuals to enter and exit at the appropriately controlled point?
- Are there security guards posted at every entrance to our organisation?
- Is the data centre secured to only allow physical access to our servers by the authorised individuals?
- Are there a proper heating, ventilation, and air conditioning systems in place?

Assessment

According to the market data, there is a gap in the market for companies providing proper security design of the physical IT infrastructure and review of services. There are utility system providers who offer fire alarms, surveillance systems, security and access systems, but most of them seem to lack an IT specific know-how. The domain requires local presence so that scalability is certainly an issue. This is the reason that business is more likely be conducted for utility systems providers.

- **Tactical interest score:** 2/5
- **Strategical interest score:** 2/5

4.10. Career development

The domain of career development involves development of cybersecurity experts by training, coaching, role modelling and certifying the domain experts. It also involves the role of being an organiser of conferences, hosting peer groups and/or other domain activities.

Assessment

Being active in cybersecurity domain and being a centre of cybersecurity experts development and peer group meetings is a compelling idea. Surely, it would enhance the organisations's brand and enable business.

Still, organisation of conferences and peer groups has a high start-up cost and a high level of customer loyalty. Changing conferences or peer groups they have used to attend to is a long process and requires years of patience (although switching cost as such is not significant).

Training and certifying of experts are much more realistic opportunities and these also relate to the User education domain. Still, career development requires certified experts and much experience and thus has a steep learning curve.

- **Tactical interest score:** 2/5
- **Strategical interest score:** 4/5

4.11. Security architecture

Security architecture (SA) is the term used to define the overall system required to protect an organisation's IT infrastructure. Security engineering is being defined as subdomain of SA, but is actually the core process of SA. It incorporates security controls into an information system so that the controls become an integral part of the system's operational capabilities and prevent the misuse and malicious behaviour.

The security subfields in focus are:

- Access control
- Secure system build
- Network design
- Cryptography
- Container security
- Cloud security

Assessment

Security architecture is specific to every organisation and requires an in-depth knowledge of your particular business, and consideration of factors ranging from the industry and company size to organisations' business model and practices. It's one of those areas organisation is willing to be hands-on rather than completely turning it over to a third party. There are opportunities to offer consultation and audit services in the field, but it does not scale well, is of a domestic nature, and has a steep learning curve pertaining a specific organisation.

The opportunities related to the domain are rather related to the specific solutions or tools that can be used as components in the architecture. E.g. routers, firewalls, antivirus software, antimalware programs, single sign on solutions, etc. Development of such solutions requires remarkable upfront investment and facing strong competition.

- **Tactical interest score:** 3/5
- **Strategical interest score:** 3/5

5. Summary

Assessments given above in Chapter 4, sorted by highest tactical scores, are shown in table Tactical domains. The more the score, the more appealing is the particular sub-domain for entering the market.

Table 1. Tactical domains

Domain	Tactical score	Strategical score
Risk assessment	5	4
User education	4	4
Enterprise risk management	3	4
Governance	3	4
Application security	3	3
Secure Architecture	3	3
Security operations	2	5
Career development	2	4
Physical security	2	2
Threat intelligence	1	5
Frameworks and standards	1	2

To indicate the results more intuitively, a wind rose diagram was compiled based on the data above. Blue line on the Figure Tactical preferences marks the tactical interest. Obviously, the higher the score, the more appealing is to enter the particular sub-domain of the cybersecurity market for tactical reasons. Branches that are most appealing, appear in the quadrants II and III of the diagram and the appeal decrements counter-clockwise.

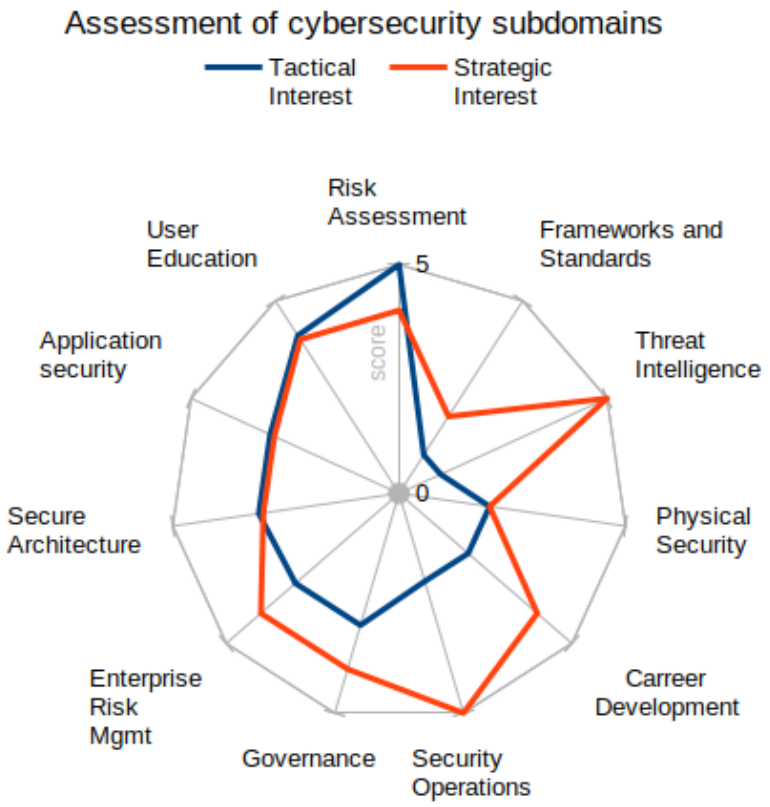

Figure 2. Tactical preferences

The strategic perspectives are different. Another wind rose diagram was compiled to indicate the appeal of the cybersecurity market from strategic point of interest. Red line on the Figure Strategic preferences marks the strategic view toards the cybersecurity market. Branches that are most appealing, appear in the II and III quadrants of the diagram while the appeal decrements counter-clockwise.

Due to different sorting, the branch labels are now placed at different locations.

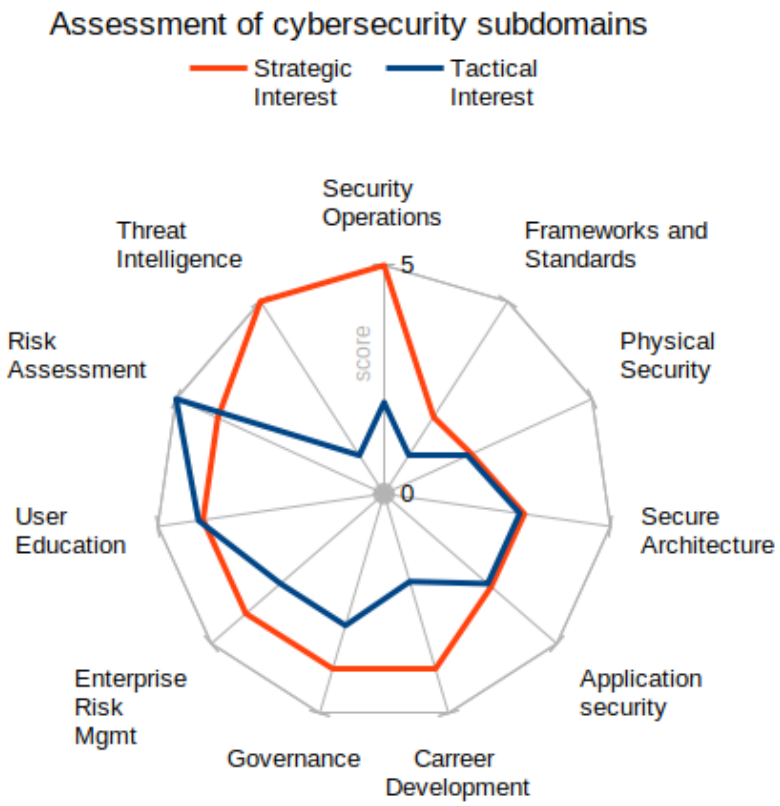

Figure 3. Strategic preferences

Two conclusions may be drawn. For organisations entering cybersecurity market on tactical grounds, the initial focuses should be on Risk assessment and User education. And then, the higher the domain on the strategic diagram, the more appealing it is for a long run and should be taken as long term goal to gain the market presence.

In the long run, the aim of an organisation should be providing an extensive range of cybersecurity services starting from the logical value chain of cybersecurity domain: Governance → Enterprise Risk management → Risk Assessment → Threat Intelligence → Security Operations → Career development and User trainings.

Despite the fact that Security Architecture and Application Security got lower scores, they still offer somewhat interesting market opportunities for companies with the appropriate skillsets.