Towards a Digital Single Market for NIS Products and Services

NOVEMBER 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use resilience@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

For providing valuable information that helped shape the report (in no particular order):

Paul Samwel, Lead Security Architect, Rabobank
Nigel Wheadon, Capability Technology Leader, Cyber, Networks Security, Data & Intelligence, BAE Systems Applied Intelligence
Kevin Bailey, Vice President – Product and Market Strategy, BAE Systems Applied Intelligence
Matthias Kaempfer, SAP Security Expert, SAP
Borja Larrumbide Martinez, Engineering Regulations and Standards, BBVA
Markku Kutvonen, Director, R&D External Partnerships, F-Secure Corporation
Johnathan Sage, Cyber Security Policy Lead, IBM Europe
Antonio Ramos, Founding Partner, LEET Security
Christopher Schouten, Senior Director Product Marketing, Nagra
Helmut Fallmann, CEO, Fabasoft AG
Fabian Bahr, Head of Berlin Office, Giesecke & Devrient GmbH
Frank Staut, CTO, SecureLink Group
Eric Lebegue, CEO Advisor, Streamwide
Pascal Beglin, CEO, Streamwide
Jan Hof, International Marketing Director, ForeScout Technologies, Inc.
Pedro Pablo Perez Garcia, VP Security, Telefonica
Prof. Theo Dimitrakos, Head of Network Function Virtualisation & Cloud Security Research European Security Competence Center at Huawei Technologies Düsseldorf GmbH Germany and Professor of Computer Science School of Computing University of Kent U.K.
Olivier Perrault, Chief Security Officer, Orange Cloud for Business

Contents

Executive Summary

A key facet of the EU's economy over the coming decades will be the consolidation of the digital market across the Member States. However, the emerging online Digital Single Market (DSM) will be in increasing jeopardy from various forms of cyber-attack. These are now growing in intensity and above all in sophistication to a level unimaginable even a decade ago.

The need for a strong and effective EU Network and Information Security (NIS) Industry becomes two-fold; on the one hand **the DSM needs protection**, which implies a strong European network and information security (NIS) sector, able to ensure protection for commercial services, the critical infrastructure and the everyday life of its citizens, who will be increasingly dependent on online services. On the other hand, **the DSM offers opportunities and tools that can be leveraged to facilitate the growth of the EU NIS Industry** with direct benefits in terms of revenue for NIS Suppliers, growth of the EU GDP and boost of employment in the cybersecurity sector; the latter is of particular importance considering the consensus that cybersecurity is one of the faster growing segments of the ICT industry.

Thus, the objective of this report is to assess the current NIS market in the EU from an economic and technical standpoint, in view of the DSM and its future demands for protection. It primarily focuses on the European market's characteristics, although key NIS offerings are expected from non-EU providers. The study focuses on five market segments – **online banking**, **online marketplaces**, **cloud storage**, **wireless telecommunications**, and **online media** – examining the cyber threat landscape, trends and the solutions provided by EU and global suppliers. A SWOT analysis identifies the strengths and weaknesses of EU suppliers as well as market opportunities and threats. In a second step, the study formulates a pragmatic industrial policy in the area of NIS, derived from the study's findings on the current state of the market, summarised in the report's recommendations to industry and policy makers.

The report's recommendations cover industrial policy and its supporting regulation, on the principle that suitable regulation will engender a vibrant EU NIS industry. Recommendations are aimed at policy makers at the EU level, with specific policy recommendations for Member States, as well as recommended actions for the EU NIS industry to advance itself. It should be noted that the proposed recommendations are in no way encouraging or enabling anti-competitive behaviour or enforcing protectionism of any kind. Instead, they are focused on **creating an environment that will foster innovation, alleviate artificial barriers** wherever possible and **optimising the use of existing tools** – in fact measures that will **generally have an equal positive effect for EU and non-EU NIS suppliers**.

Recommendations for **EU Policy Makers**:

- **Conduct a needs analysis** with in-depth examination of the objectives of the industrial policy, based on the risks due to technological dependence on ICTs and their consequences
- **Increase awareness of the market and change behaviour** to stimulate demand for NIS products
- **Focus R&D planning** on supporting the development of innovative ideas and technologies in the cybersecurity domain and to strengthen their **link to the EU cybersecurity industry**.
- **Support the industrialisation** of new offerings and technologies following the R&I phase
- Support the **creation of industrial clusters**
- Increase the footprint of **dedicated NIS operational support centres**
- Promote **EU-level harmonisation on certification** of NIS services and products
- Enhance the relevant **regulatory framework to ensure protection of countries, companies and citizens while remaining strongly business-oriented**

Recommendations for **National Policy Makers**:

- Introduce public procurement policy to **support SME NIS suppliers at a National level**
- Foster the **creation of innovation clusters** at a National level, bringing together start-ups, SMEs, academia, research centres etc.
- Draw **national guidelines for cyber protection** for each industrial sector
- Follow a **risk-based approach on national critical infrastructures** and set a mechanism to monitor cyber security readiness levels
- Promote **NIS training and educational measures** with emphasis on producing a new, highly qualified NIS workforce

Recommendations for the **NIS Industry**:

- **Build on its advantage in the context of Data Privacy and Trust** by focusing on products that cover the GDPR needs
- Explore **cyber-insurance as a driver for stimulating growth in demand** and for raising awareness
- Push for **standards**, first at EU level and ultimately for global standards
- Push for **harmonised certification across all Member States**
- On the user company side (Demand Side), **cybersecurity should be a concern at board level of all companies**
- **Develop a global mind-set** when setting its goals for growth potential and explore possibilities available outside the EU Market
- **Build the NIS ecosystem**, as the market is moving towards holistic solutions covering the supply chain

1. Introduction

The importance of the Digital Single Market (DSM) to the EU economy and society is such that its protection from cyber threats is critical. This study by ENISA examines the need for cybersecurity protection in the DSM in order to ensure its growth, trends in the threat landscape, and the market for network and information security (NIS) products and services in the EU to meet those needs. With its focus on the EU market, the study's scope was to cover both supplier views and the end-user perspectives in selected market segments, taking into account the impacts of NIS offerings from non-EU providers.

1.1 Scope and Objectives

In the context of the study, the scope of NIS products and services – or the NIS market - is defined as including all products and services that protect the ICT assets and operations of consumers and companies.

Due to the extensive scope of the DSM, the present study scopes down the analysis to the following **five selected market segments**. The rationale for selecting these segments is briefly described in Section 2.

- Online banking
- Online marketplaces
- Cloud storage
- Wireless telecommunications
- Online media

Aimed at a target audience of **policy makers in the European institutions**, **EU Member States** and the **EFTA nations** as well as **senior management in the private sector**, the study makes recommendations to support the development of a more effective European NIS industry to protect the DSM. The objectives of this study are, thus three-fold:

1. **Understand which NIS products/services are successful** in 5 specific market segments and how EU suppliers are positioned (and why)
2. **Find ways to improve the growth and market penetration of EU suppliers** by leveraging the opportunities and tools available within the DSM
3. **Propose recommendations for development of a more effective European NIS industry** to both protect the DSM, but also benefit from the opportunities and tools available within the DSM

1.2 Policy Context

The increase in cyber threats and the perception of cyber insecurity is causing a growing mistrust in citizens, potentially holding back the European economy as it increasingly becomes digital. Recognising its key importance to growth of the EU's digital economy, cybersecurity forms a key component in the European Commission's **Digital Single Market** (**DSM**) **strategy**.[1]

The DSM strategy recognises the need to protect the EU's communication networks and critical infrastructure and respond effectively to cyber threats, and the need to build on existing national and EU-level cybersecurity strategies and regulation. The DSM strategy reiterated the **EU's 2013 Cybersecurity**

[1] A Digital Single Market Strategy for Europe {SWD(2015) 100 final}, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf

Strategy[2] and also announced a plan to establish a **Public-Private Partnership on cybersecurity** (**cPPP**)in the area of technologies and solutions for online network security, which was launched in July 2016.[3]

The aim of the EU's Cybersecurity Strategy is to establish common minimum requirements for network and information security (NIS) among the Member States; to set up coordinated prevention, detection, mitigation, and response mechanisms; and to improve the preparedness and engagement of the private sector. The strategy seeks to stimulate demand for effective NIS ICT products and to certify these products by establishing a platform to identify good cybersecurity and by developing security standards for cloud computing.

In particular, the DSM strategy also highlighted one of the key priorities of the Cybersecurity Strategy, which is to **develop industrial and technological resources for cybersecurity**, acknowledging that gaps exist between the rapid development of technologies and solutions for online network security. It calls for "a more joined-up approach… to step up the supply of more secure solutions by EU industry and to stimulate their take-up by enterprises, public authorities, and citizens".

The Commission is now considering[4] key activities to protect the EU against cyber-attacks covering multiple aspects, such as supporting EU NIS R&D and innovation for increased competitiveness[5], prompting European cooperation for a series of Sectoral Information Sharing and Analysis Centres (sectoral ISACs), removing barriers that prevent market participants from sharing event information and more.

The adoption of the **Directive on Security of Network and Information Systems** (**NIS Directive**)[6], in July 2016[7] marks an important step forward, obliging Member States to adopt their own national cyber security strategy, mandating Computer Security Incident Response Teams (CSIRTs) in each Member State and foreseeing the creation of the CSIRT Network for their tactical/operational coordination. Importantly, the Directive includes requirements for cooperation and information exchange between the European Commission and the Member States.

In terms of Data Privacy and Data Protection, the new **General Data Protection Regulation** (**GDPR**)[8] is set to replace the **Data Protection Directive 95/46/EC**[9] effective May 25, 2018. The GDPR is directly applicable in each member state and will lead to a greater degree of data protection harmonization across EU nations. The GDPR is an important step forward for enhancing privacy of EU citizens, harmonizing data protection rules across Member States, and promoting privacy and security as core aspects of the European industry.

---

[2] European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy for the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667

[3] http://europa.eu/rapid/press-release_IP-16-2321_en.htm

[4] Communication on *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*, COM(2016) 410 final, 5 July 2016, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16546.

[5] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16545

[6] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[7] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[8] http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[9] http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=celex:31995L0046

The **Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market**[10] (**eIDAS Regulation** - electronic IDentity and Authentication Systems Regulation) was adopted by the Council of the European Union on 23 July 2014. This new regulation establishes a new legal structure for electronic identification, signatures, seals and documents throughout the EU. Several implementing acts have been adopted by the **European Commission** on electronic identification and on electronic trust services[11]. The eIDAS regulation pertains to electronic signatures and aims at ensuring confidence in electronic signatures and creating mutual recognition of electronic signatures across all member states. Specifically, it regulates electronic signatures, electronic transactions, involved bodies and their embedding processes to provide a safe way for users to conduct business online, a critical facet of ensuring trust in the DSM.

In summary, the expected benefits of a cybersecurity policy for citizens, enterprises, governments and consumers in the DSM are outlined in Table 1.

Table 1: Benefits for the EU Economy and its Citizens of Suitable NIS Policy

INITIATIVE	BENEFITS FOR CITIZENS, CONSUMERS AND BUSINESS
Cybersecurity Strategy	Outlines the EU's vision and the actions required, based on strongly protecting and promoting citizens' rights, to make the EU's online environment the safest in the world.
NIS Directive	Proposals on risk management and reporting of security incidents mean that citizens and consumers will have more trust and confidence in the technologies, services and systems they rely on day-to-day.
General Data Protection Regulation (GDPR)	Will strengthen citizens' rights and helps restore trust. Citizens can be more confident about how their personal data is treated, particularly online. Citizens will have more control of their data, notably through: the right to be forgotten; easier access to their own data; consent on how their data is used; and the right to know when their data has been hacked.
E-Privacy Directive	Sets out fundamental rights and freedoms of EU citizens when using electronic communications, including information for consumers on data breaches and improving enforcement.
Safer Internet Programme/Better Internet for Kids	Children will benefit from better digital and media literacy skills and more creative and educational online content. Parents and children will benefit from better ways of staying safe online, such as simple, effective tools for reporting abuse, age appropriate privacy settings, content classification schemes and parental controls.
E-Inclusion policy	Aims to reduce digital divides by targeting older people, the economically inactive, those with lower levels of education, and people with physical disabilities by reducing the number of people who do not use the internet regularly, increasing broadband penetration, improving basic digital literacy skills and improving accessibility.
Trust services and E-ID	Boosts trust and convenience for consumers in cross-border and cross-sector electronic transactions; sets standards for e-signatures and approval labels for services.

1.3 Methodology

Information collection was done directly from the NIS market in the EU via engagement of the relevant industry stakeholders, namely

- Major **NIS users** from the five selected market segments, who provided insights on the *Demand Side* for NIS products and services

[10] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN
[11] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

- **Suppliers of NIS products and services** collectively covering a very broad scope of the NIS offerings and comprising leading and smaller NIS suppliers; they provided insights mainly on the *Supply Side* but, due to their profound understanding of the customer landscape, also supported the data collection regarding NIS product demand.

Most information was collected by a series of over 20 in-depth, non-attributable structured **interviews** with representatives of the aforementioned stakeholder groups, while an **online survey** was also published. Their information was gathered under condition of non-disclosure, which encouraged full and frank exchange of views and expert opinions, giving insights into a sector that has yet to be examined closely as to structure and future directions. The information collection was supplemented by **desk research** which also covered reports from leading market analysts, as well as a variety of published sources.

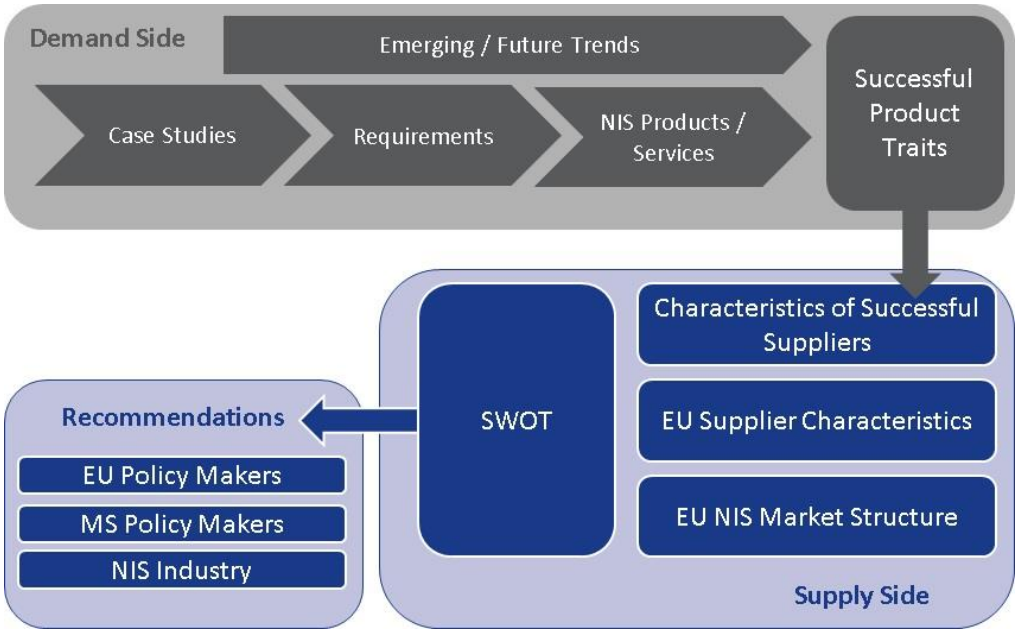
Finally, two study meetings were held:

- A **work meeting** in the École Militaire in Paris under the auspices of L'institut national des hautes études de la sécurité et de la justice (INHESJ), with some twenty invited NIS players, both suppliers and user organisations.
- A **validation workshop** in Brussels hosted by the European Commission with representatives of NIS Users and NIS Suppliers, where the study findings and recommendations were presented.

The approach to the study, particularly the way in which the information collected for the Demand Side and the Supply Side was analysed, is depicted in Figure 1. The analysis approach was the following:

1. **Demand Side Analysis**
    a. Analyse **Case Studies**, i.e. application areas to protect in each market segment and key threats
    b. Document **Requirements** in terms of cybersecurity deriving from the case studies
    c. List **NIS Products / Services** that are most broadly used in each market segment
    d. Assess **Emerging / Future Trends** in terms of technology, business models / case studies, threats etc. to integrate the Demand Side dynamics in the analysis
    e. Produce a list of **Successful Product Traits**, i.e. what makes a product/service successful
2. **Supply Side Analysis**
    a. Map the Successful Product Traits to **Characteristics of Successful Suppliers**
    b. Document the **EU NIS Market Structure** in terms of current characteristics and evolution to understand both its internal mechanisms and how it compares to the Global NIS Market
    c. Map the **EU Supplier Characteristics** to understand their respective positioning in the EU and Global NIS Markets
3. **SWOT Analysis** for EU NIS Suppliers based on a synthetic analysis of all Demand Side and Supply Side findings
4. **Recommendations** towards
    a. EU Policy makers
    b. Member State Policy Makers
    c. The EU NIS Industry

Figure 1: Analysis Approach



1.4 Structure

Following this introduction, the rest of this document is structured to reflect the Analysis Approach presented in Section 1.3. Hence:

Chapter 2 presents the Demand Side for NIS Products and Services, focusing on products with horizontal applicability, specific requirements and assorted products for each of the selected market segments based on concrete case studies and application areas and, finally, characteristics of successful products and services.

Chapter 3 presents the Supply Side for NIS Products and Services, analysing the EU NIS Market in terms of structure, offerings and evolution, the Global NIS Market and its comparison to the EU Market, the emerging trends that dictate the dynamics of the NIS industry in terms of offerings and structure and, finally, the characteristics of the successful NIS suppliers in the EU.

In **Chapter 4**, a SWOT analysis reveals the strengths and weaknesses of the EU NIS industry, combining the key findings and conclusions of the Demand Side and Supply Side analyses.

Finally, recommendations are given in **Chapter 5** for policy makers at EU and Member State level and for decision makers in the private sector.

2. The Demand Side for NIS Products and Services

We have examined the NIS market from the user viewpoint, focusing on specific market segments for deeper analysis to better understand the cybersecurity issues and threats facing the EU economy.

These market segments are examined as specific case studies – with commercial applicability – to determine the respective requirements for NIS products and services, the corresponding NIS products and services needed for their protection and the characteristics of the products most successful within this scope. The rationale behind selecting these five market segments was the following:

- Represent Critical Infrastructures, which will provide the right environment for the DSM. In this context, the Telecommunications sector was selected for its pertinence and, due to its very broad scope, was scoped down to **Wireless Telecommunications** (providers and manufacturers of equipment).
- Represent commercial applications of Critical Infrastructures mapped to the Operators of Essential Services as defined in the Directive on Network and Information Security (NIS Directive). In this context, **Online Banking** was selected.
- Represent Digital Service Providers as defined in the NIS Directive. In this context, **Online Marketplaces** were selected, also due to their pertinence to the first pillar of the DSM ("improved *access to online goods and services*").
- Represent Cloud as a horizontal technology spanning across multiple aspects of the DSM, and also identified within the context of Digital Service Providers. In order to narrow the scope, **Cloud Storage** was selected.
- Finally, **Online Media** and, particularly, video streaming was selected as a service that is expected to grow significantly over the next few years in the EU, judging by its current footprint in the US market.

This demand side analysis focuses on the following aspects:

1. **Case studies** for commercial applications and the respective threats
2. **Security requirements** deriving from the case studies
3. **NIS products and services** needed to meet said requirements
4. **Emerging / future trends**, which should always be addressed in the context of market studies as they provide an overview of the dynamics and evolution of the demand side
5. **Characteristics of successful products and services** combining the aforementioned aspects into concrete traits that determine the success, or lack thereof, of NIS products and services in any given segment

One of the findings of our research with users and suppliers was the similarity of attack profiles against the different types of vertical users as well as the solutions employed. While there are some differences between market segments, they are characterised more by their similarity in terms of NIS products and services needed for their protection. Moreover many NIS product and services categories have broad niches within the generic label, not offering specific solutions per sector.

There is a broad range of NIS products services with a horizontal applicability, driven by threats that are common across multiple market segments. These threats include:

- Malware attacks, through worms and viruses

- Denial of service attacks using botnets for flooding the network
- Data breaches aiming at stealing credit card details
- Identity theft (spoofing) and fraudulent online transactions
- Ransomware attacks that encrypt any visible files.

Threats are expanding in sophistication, so today, we could be dealing with combinations of types of the aforementioned attacks. These are called Advanced Persistent Threats (APT) and require special handling to mitigate the impact they cause.

Hence, classification of NIS products and services may be done by:

- The **threat type** that the product or service is designed to handle, for instance intrusion detections systems (IDS) and intrusion prevention systems (IPS);
- The **attack target**, for example, user terminal devices (endpoints) or servers or databases.
- The **vertical industrial segment** that is being targeted, for example, online banking, cloud storage, Internet of Things (IoT), online media, and so on.
- Etc.

Thus an overall indicative market classification along five dimensions – that integrate the aforementioned aspects and address complementarities and overlaps - is shown below:

- **Target elements for attack**: Network (WAN, WLAN, LAN, mobile); Data centres; Servers and server farms; Databases; Endpoints, devices; Applications; Cloud infrastructure and services; Network operations centres; Call centres; and so on.
- **Network user configuration**: Private multi-user; Corporate network (Intranet-Extranet); Public mobile; Private cloud; Public cloud; VPN; Public Protection and Disaster Relief (PPDR) services; Public Wi-Fi; and so on.
- **Product category**: Identity and Access Management (IAM): Security intelligence and event management (SIEM); IDS/IPS for intrusions; Firewalls; Encryption; Threat intelligence; Antivirus; Endpoint protection; and so on.
- **Service category**: Managed security service; Incident alerts; Risk audits with financial impacts; Restoration; Product/service certification; Threat intelligence gathering; Systems Integration (S/I); Training; Attack testing with systems breaking; and so on.
- **Major types of target networks**: Web services and web farms; EPOS/cards/ATM; Industrial/IoT; Web and cloud services; Mobile RAN and core; Fixed broadband; Wireless telecommunications; Content distribution networks; Online marketplaces; PPDR networks; Sector networks (e.g. SWIFT); and so on.

The following section draws on the findings of a programme of in-depth interviews with representatives of each market segment and NIS suppliers, supplemented with desk research, to highlight the needs of the five selected market segments by threat type, targets for attacks and solutions

2.1 Online Banking

2.1.1 Threat Types

Two main threat mechanisms are seen in the online banking sector:

- **Loss of availability** was mentioned during the interviews as a key threat. **Denial of service attacks**, with this aim, are experienced quite often – typically a bank might experience such attempts two or three times per month. However through using filtering (IPS/IDS and firewall systems), this type of threat is

becoming less of a worry to many banks. Levels of high traffic overload can be handled more easily than in the past, and many banks are now prepared for higher load attacks.

- **Impersonation attacks** (spoofing, sniffing, masquerading etc.) are the second major threat that all banks must deal with, in addition to attacks on a bank's internal systems. **Manipulation for fraud**, by examining the database of transactions – the transaction ledger – is now widespread in tracing customer transactions for fraudulent purposes. The banks often see **social engineered attacks** and the threat level here is increasing. Clients are often manipulated by such socially engineered attacks as phishing but less within banks.

- **Injected malware**, e.g. through calendar meeting arrangers especially outside or through attachment in emails, in the business client base.
- **Virus infections** are not the only common malware seen as **network transported worms** are common.

These threats must be seen against the background of the banking industry which has legal compliance regulation on maintaining operational continuity, i.e. uninterrupted business, as well as safeguards on data security and privacy. That makes solutions less cost sensitive to some extent.

2.1.2 Application Areas to Protect

Key targets may be on external or internal bank systems. In terms of external systems, the **clients' end point devices** are the major target, most often on **mobile banking interactions**. Attacks are more sophisticated, and can target the mobile phones which is used for two-factor authentication purposes.

The main internal areas attacked are:

- **Databases** - the most common; better detection and protection is required now
- **Networks** are the second prime internal target
- **Office systems** may be an attack target

Although some banks are now considering **cloud-based storage and transaction processing**, opinions differ on their security risk. Cloud security is often considered a weakness. Thus many banks will not yet use cloud-based databases, transaction operations or application hosting.

2.1.3 Solutions

NIS products and services demand in the online banking sector is, to a great extent, driven by the banks' regulatory compliance, which now includes:

- The European Central Bank (ECB) rules via the Single Supervisory Mechanism (SSM) Framework, which has cybersecurity provisions and since November 2014 forms a key part of the banking regulations for the Eurozone.
- Treatment of cybersecurity incidents, which is expected to come under new scrutiny from the ECB as it expands the SSM in 2017. The banks tend to have already built some form of a perimeter of security that protects all their internal systems, networks and databases.

Such a perimeter structure follows a mitigation technique focusing on two kinds of threats – those from external sources, usually from the internet – and the insider threats, inside the bank's operations:

- Layered defence, namely setting up firewalls (packet inspection) and IPS/ IDS to create zones of security in the system. Also using secure networks for data transaction is another common solution.
- Operation security techniques, such as **isolation of malicious intruders** is also beginning to be used by some, to trap and then examine data within a transaction. Thus the external client must wait while the examination takes place.

- Application security techniques, for example some banks use **white-listing of applications** for countering certain types of mobile device fraud/attacks.

In these conditions some threats still exist such as social engineering attacks on senior staff especially via email but these can be handled by suitable **education and training of staff**. But now threat mechanisms are developing so fast that banks need new tools – and not point products but an interlocking set. That should form a security perimeter that can far better protect operational systems within the organisation. It might include:

- More **advanced AI techniques** for attack and malware detection. Many banks have looked at AI tools for anomaly detection, which review transaction and network activity using behaviour-based algorithms for incident detection for abnormal behaviour on both internal bank and the customer side of events. However machine intelligence today cannot safely identify fraud, an attack or an anomaly in customer behaviour but human intervention can be far more effective and safe – false positives in cases of AI may also be an issue here. Such **machine learning tools for attack detection, prevention and managed restoration** are needed by the banking industry today. Existing tools may not meet EU standards for data and privacy compliance.
- Also banks would like **internet banking channel-monitoring tools**. This could be outsourced to an external specialist as a service.
- **Intrusion and malware detection tools** that are improved over current offerings with indicators of compromise for networks and services are needed.
- **Tools for monitoring insider malicious actions** and activities against pre-set rules are also required.
- A key area for future NIS product/service spend will be in **business recovery**. This process comprises all the actions to restore the original operating environment with the latest uncompromised data.
- Banks would also like **tools that assess the level of security**. These would have to be linked to banking industry priorities for business protection. What is needed are two advances, in:
    - How to **assess security levels for a whole bank**, and
    - How to **standardise security protection levels** so they can be **compared across multiple banks**. Comparative measures of a bank's protection levels against compliance and those of other banks is a key requirement.

Cloud based operations might be used in the future but banks need complete security ratings for such hosting. The concept of a private cloud for banking is seen by some as the best way forward. Use of public cloud service providers is seen as too risky by some banks, as it is assumed that they would become a new attack target for the most sophisticated banking criminals, such as those that performed the EFT fraud on SWIFT in 2016[12].

2.2 Online Marketplaces

2.2.1 Threat Types

Online payment systems associated with online retail and ecommerce markets have been the subject of increasing fraud over the past decade. Financial gain is the key motive. The majority of attacks occur at two levels:

- At individual customer level (often using **phishing**) for **exploiting individual customer transactions**. Here the attack surface of mobile smartphones has had a major impact, e.g. with downloaded apps

[12] Townsend, K., (2016) Second SWIFT attack hits Vietnam bank showing links to Sony hack, Security Week, 13 May 2016, www.securityweek.com/second-swift-attack-hits-vietnam-bank-showing-links-to-sony-hack.

- **Data breaches at major corporate database level** for theft of customer account details including debit/credit card data (e.g. the 2013 Target Corporation attack in the USA that exposed 40 million cards) as well as internal fraud or partner fraud (e.g. the InComm example of PayPal's cash card partner[13]) by employees. These may also include data breaches in point of sale terminals

A 2015 survey[14] in the USA noted that web application attacks hit retail applications the hardest. Table 2 identifies many of the types of online attacks for fraudulent purpose ranked by the levels of concern of merchants in six countries,[15] with mobile identified as the latest major threat vector.

Table 2: Online Markets – Main Fraud Levels[16]

BIGGEST FRAUD CONCERNS FOR MERCHANTS	BIGGEST MOBILE RISK FACTORS, IN MERCHANTS' VIEW
Identity theft – 71%	Malware on mobile devices – 51%
Phishing and related social engineering – 66%	Spyware on mobile devices – 46%
Account takeover – 63%	Unsafe network and data connections – 46%
Various types of payment fraud – 61%	Consumers losing their mobile devices – 43%
Botnets – 50%	Insecure apps/ applications – 34%
Man in the middle attack – 28%	Consumers using mobile transactions with unsafe practices – 34%
New threats not yet seen – 4%	Malware on mobile devices – 51%

A specific series of threats apply to online shopping, with nine types of attacks most likely:[17]

- **Dos** through **Botnet** – brings down its websites
- **Mobile app store fraud** – manipulate rebates
- **Mobile device** – key logger account takeover
- **Click fraud** – false customer clicks in online ads
- **Testing stolen credit cards** – validate if active
- **Spear phishing internally** – hijack accounts
- **Electronic wallet intro** – exploit lack of controls
- **Mass registration** – spoof website – customer data
- **eCoupons** – accumulate discounts falsely.

Typically attackers use:

- **Key logger malware** at the individual customer level to steal card details on a mobile smartphone or tablet, including any supplementary security keys.
- At the corporate level of the retailer, various forms of **APT** have been seen, such as **DDoS** combined with simultaneous **intrusion for data theft**, using **SQL exploits**.

[13] https://www.igobyplane.com/2016/05/16/billion-dollar-paypal-my-cash-scam-partner-incomm-scam-got-busy-victim-blaming-me-while-i-got-busy-finding-their-fatal-security-flaw-and-embezzlers/
[14] Imperva Web Application Attack Report, 2014/2015, https://www.imperva.com/DefenseCenter/WAAR.
[15] UK, USA, Japan, China, Russia, India.
[16] Worldpay (2014), "Fragmentation of Fraud: A unique view on International eCommerce fraud".
[17] Ponemon Institute (2013), "The 2013 eCommerce Cyber Crime Report: Safeguarding Brand and Revenue this Holiday Season", Ponemon Institute Research Report, October.

As the different types of schemes increase, a fragmentation of payment methods is occurring, and with it, a loss of confidence in the ability to manage fraud across multiple payment methods and channels. For EU online retailers, there are a number of **unique challenges for operating across multiple Member States**, requiring a comprehensive approach to tackling fraud:

- **Integration of cross-border systems**, but many retailers lack a holistic oversight policy
- **Gathering all data for authentication** with a single view of the customer (the KYC problem)
- **Increasing volume of transactions**, and fraud in specific countries, possibly undetected
- **Difficulty with foreign fraud management tools** complicated by language differences.

2.2.2 Application Areas to Protect

Four main centres of attack stand out:

- **End point devices** mainly consumer devices - mobile phones and laptops
- **Data Centre breaches** for customer banking details
- **Networks**, especially mobile, e.g. via the RAN for man in the middle attacks
- **Point of sale terminals** in merchants connected to the web.[18]

The online sales channels perceived to be most prone to fraud are shown in Table 3.

Table 3: Online Sales Channels Most Prone to Fraud[19]

CHANNEL	% OF MERCHANTS PERCEIVING A RISK
Online sales through third party website	69%
Mobile commerce - m-commerce of any kind	64%
Online website	55%
Partner / sales agency / broker sales	39%
Call centre	36%

2.2.3 Solutions

In surveys of online retailers, the main tools and tactics used to prevent fraud are:

- **Validation services** (93%) or proprietary/customer data (83%).[20] Solutions for validation of services are usually basic, with the **two factor authentication** still used for card-based online transactions in Europe, i.e. some form of card identity plus a personal code to identify whether the card is actually present.
- Highly imperfect, online systems with card not present (CNP) have the most prevalent fraud. In response, online payments services such as PayPal have resorted to their own **AI solutions** in proprietary systems that **monitor transactions for anomalous behaviour**.[21]
- **Endpoint security for mobile devices** wherever possible, with **encryption of transactions** as well as the **encryption of customer and transaction details** held on the user devices with all customer databases encrypted within the retailer, with effective **key management**.

[18] US Computer Emergency Readiness Team, Malware Targeting Point of Sale Systems, Alert (TA14-002A), https://www.us-cert.gov/ncas/alerts/TA14-002A.
[19] Worldpay (2014), "Fragmentation of Fraud: A unique view on International eCommerce fraud".
[20] Worldpay (2014), ibid
[21] Morisy, M., (2016) "How PayPal boosts security with artificial intelligence", *MIT Technology Review*, 28 January 2016.

This difficult fraud management situation requires solutions for a fragmented payments landscape, so any **fraud-prevention/detection tools** should cover all types of payment method transactions, not just cards. Partnership with a fraud examiner is considered essential to keep abreast of new threats. NIS product solutions are difficult to apply because so much depends on a customer base that is outside the retailer's control in NIS terms.

2.3 Cloud Storage

2.3.1 Threat Types

Trust is key for all players in the supply chain based on a cloud service, as this engenders loyalty. In the EU, the trend is towards an equal importance for privacy. A "trust chain" can be observed with cloud storage.

Thus, complete security is viewed as a de facto requirement for cloud services and the trend is to mounting levels of security. However a significant administrative drawback may be the cloud SLA. Traditionally, cloud service providers (CSP) may have taken a "hands off" approach to security. Effective and consistent SLAs, which change with time and are often designed to protect the cloud service provider rather than the service consumer have been in use. The focus on a new generation of cloud SLAs has moved the weight of responsibility further towards the cloud service providers but more is expected.

For cloud-based threats focusing on cloud storage, the primary concern is **theft** and **compromise of customer data** but others include **loss of governance**, **failure to respond to SLA requirements**, **isolation of failures**, etc., analysed in the ENISA Threat Landscape.[22]

2.3.2 Application Areas to Protect

Attacks on cloud storage services are aimed in order of priority at:

1. Cloud-stored database;
2. Their connecting networks and virtual machines;
3. The hosting data centres.

Today, the protection situation for cloud storage providers is complex. Too often it consists of extensive use of globally dispersed, heterogeneous protection services, often managed by multiple independent organisations. So cloud security may be porous, as it has major difficulties with:

- Monitoring all the external interfaces and traffic across a **complex global server farm**
- Ensuring all the many different OS types and releases and applications have **up to date patches**, throughout the infrastructure
- Assigning **responsibility for protection failures** with the numerous providers or customers (in case of IaaS or PaaS)
- The **hypervisor can be a vulnerable aspect** as a single point of failure or corruption.

Significant reliance on virtualisation means that hypervisor security and management is key to security of cloud services[23]. In particular, control of the hypervisor in a cloud environment is a point of tension between the CSP and the customer as currently the CSP retains control (SaaS) while, in some cases, the consumer

[22] ENISA Threat Landscape, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape.
[23] https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

would like control (IaaS). There is also a **trend for cloud attacks to move "up the stack''**, i.e. attacks are exploiting application level vulnerabilities (SaaS) rather than those of the underlying network (IaaS). Moving down the stack makes the Cloud more secure, but the provider less responsible. For the simpler network case, adequate protection may come from a conventional firewall that performs the same task regardless of the service being provided.

2.3.3 Solutions

Secure cloud storage requires a clear view and understanding of the service provision supply chain, i.e. the attack surface. Threats may be vertically based to some extent and hence solutions may be customised or tuned, or accredited, for different vertical sectors, e.g. health. The most significant threat identified by CSPs is a data breach (as Cloud is resilient to loss of availability). Increasingly, commercial organisations state that they use **encryption** within networks for data in transit and for data at rest in databases. Greater use of encryption and **digital signature services** to address threats in a progressively more dispersed cloud infrastructure is a growing trend and a user's requirement. There are a number of encryption issues that need to be addressed in a cloud environment:

- Ensuring the keys **required to encrypt data are stored and managed in a secure manner** while access to their use is highly restricted in an auditable manner.
- Ensuring **appropriate encryption is applied throughout the data life cycle**, i.e. data backup, data reporting dumps, transfer to removable media. Database encryption should such that it does not impair the search function but maintains the confidentiality of the data stored.

Today there is a **lack of effective tools or infrastructure services that simplify the implementation of encryption, digital signature services and key management**. So implementing them at the application level is complex. Such measures have to be capable of applying a range of algorithms, profiles for application, key management and storage scenarios, and data recovery requirements. Moreover, increased reliance on hypervisors requires further study on vulnerabilities particularly in different operating environments.

In order to achieve **input validation** (for cloud storage) increased use of **analytics to monitor traffic** and **monitor and recognise attacks** is favoured by some technology vendors. To be effective, hooks for analytics need to be built into the different layers of the IT stack and exposed to the NIS analytic tools in a secure fashion so that all of the attack surface, which may be provided by multiple organisations, can be monitored. Separate monitoring "silos" operated by different organisations disrupt an integrated response aimed at managing security in a holistic manner across the client's supply chain.

For cloud storage providers and their clients, all of this is particularly challenging given the scale, geographical and heterogeneous distribution and the fact that different organisations may be responsible for different platforms. **Improved automation** is a strong requirement for effective secure management of cloud storage. For instance, the banking industry wants to be able to monitor the overall security level of a cloud-based service, before investing in such initiatives. Part of this may be a cloud service security broker (CSSB), which can establish and monitor service relationships in real time, to ensure that required security policies are enforced.

2.4 Wireless Telecommunications

2.4.1 Threat Types

Threats are changing with the scale of systems. In general, a growing threat is the loss of control owing to the very magnitude of systems being dealt with. Any IT service provider has to manage much more today –

a huge attack surface. Cloud services expand this, as many different server types are called for and these may have to be widely dispersed, perhaps globally. Also, for the Internet of Things (IoT) that is coming, and its potential scale, management of communications over the Internet is difficult to perform securely.

Introduction of SDN (Software Defined Networks) with NFV[24] (Network Functions Virtualisation) are already changing the threat vectors for carriers. Such **APT** may make it possible to create a nationwide hazard and could be difficult (and expensive) to detect. This form of stealth attack would tend to bypass the current underlying NIS protection strategy. They may be undetectable at a network level, and overall, difficult to spot and identify as a complete attack, as its authors would act outside the typical context of more normal threat patterns. Such attacks would require privileged access at many different levels, e.g. by dispersed incidents at different levels that are (deliberately) difficult to link up as one attack.

But the key threats lie outside the telecommunications operators, i.e. in the **customer base**. Moreover the proliferation of **mobile devices** (smartphones, tablets, laptops) their online use creates massive threats, also situated outside telecommunications operators, especially as patches and updates are poorly observed. This vulnerability is particularly true in SMEs who also lack trained staff, and who have a poor corporate level attitude to, and awareness of, cybersecurity. A key area of vulnerability toady is **smart apps for mobile devices**, which act as a broad attack vector.

Ransomware is a rising threat. Other threats include **security risks from third-party outsourced service providers**, where **data security** can be a problem, especially if it touches internal administrative data or the customer data. For instance, use of overseas call centres can be major **data privacy** problem when outsourced overseas to third parties.

In general in the telecommunications sector, market offerings for cloud services are also used internally by other divisions in a company. To protect the data centres hosting its cloud services, most operators now have their own internal security teams and their management buys in appropriate products on the NIS market. Thus in general, the most prominent threats for the operator are:

- **Phishing attacks** which are multiplying: social engineering especially in the customer base for malware penetration is perhaps the largest threat
- **Back doors or security holes** due to lack of updated security patches for packaged software is a major problem, especially with the scale of the operations and the dispersion of data centres, perhaps globally
- **Fraud** particularly theft of customer financial account details (e.g. TalkTalk)
- **DDOS attacks**, e.g. blocking emergency services numbers
- **Man in the Middle** attacks, a network threat generally.

So far we have examined the mobile network operator side. However, manufacturers of wireless telecommunications equipment, including chipsets, focus more on the **intellectual property aspects**. Their vulnerabilities both internal and via third parties are numerous. They see their **staff** in the front line for many of today's attacks at a personal level (**phishing**, **malware**, **ransomware**, etc.).

[24] SDN and NFV provide flexible low cost networking by presenting the network functions in software. Thus the physical outside switching fabric is minimised as many network functions are hosted in remote data centres. That gives complete flexibility over networking configurations, protocols and to some extent data rates and overall capacity. Naturally that also adds network vulnerabilities to cyber attack as the network management and operation is no longer "hardwired" in equipment but is a software construct that can be maliciously manipulated.

2.4.2 Application Areas to Protect

Attack targets in approximate order of severity are:

- The **databases**
- **Front-end systems**, especially call centres
- The **wide area networks** for broadband service for Internet connection and mobile core fixed line operations with the MNO RAN (Mobile Network Operator – Radio Access Network)
- **Web farms**
- **Data centres**, which have an increasing threat with NFV/SDN
- **Internal office systems** (and all internal central services).

What is new for the telecommunications industry is investments in the **IoT**, where many EU operators are spending significantly. A further new area is the digital workspace, i.e. **virtualisation of the desktop** (**VDI**) and all work on a computer for a client company and its staff. The general trend is for all enterprise IT to be entirely outsourced. That includes mobile working and integration of mobile devices and the industry is already serving this market.

While cloud and IoT are the current application trends for the MNOs, the trend is to invest more in 5G and NFV/SDN over the next five years. The new threats introduced are quite varied. For mobile operations, the threat depends on **what is on the device**; 5G implies far **more data** while the magnified bandwidth on the endpoint device, increases the threat level. The attack surface has increased with NFV and SDN and so there needs to be verification that the virtual networks nodes "said to be in use" can be **trusted** as not being a false set that guides traffic elsewhere, maliciously. So authentication of configuration patterns will be the next demand from the industry.

For the equipment suppliers, **the key target is the intellectual property**, so access to databases of designs, tests, research projects and technical strategy are the key targets. But application areas to protect are not just the data stores but also the **staff** as it is through social engineering that unauthorised access is commonly made.

2.4.3 Solutions

- Users are in the front line for many of today's attacks (phishing, malware, data ransom, etc.). Hence, **user awareness** is a key weapon in the fight against cyber attacks.
- Highly scalable security systems, able to secure and check the largest implementations (firewalls, IPS/ IDS). That implies forms of **automated, autonomous security** – not just for intrusion protection but also for maintenance procedures such as **verifying all software release status** and **applying updated patches on an enormous scale**. Autonomous security maintenance systems for world scale networked systems are difficult to implement.
- The industry sees that for future NIS development, the key area is AI – for new tools, with the ability to leverage **security teams in a security operations centre**. So tools would be would be **SOC (security operations centre) based** with modelling as well as alerts and analysis to optimise threat protection processing.
- MNOs have already developed their own **analytics tools based on AI** for attack alerts and to help their internal security teams respond faster. AI may be positioned as an additional analytic layer, on top of the layered architecture of "point" NIS tools, or, integrated within the tools. The MNOs' latest tools may use **visual analytics for interactive use with probability weightings**. Integration of security teams with AI tools has now evolved sufficiently for the human analyst to be part of the analysis loop, which makes a much stronger link – essential for **real-time working/decision taking**.

For the telecommunications equipment and chipset manufacturers, the front line for information access is often social engineering aimed at members of staff. Hence, user education is a key weapon in the fight against cyber attacks. To be at all successful in training, the companies involved expend much effort, planning and good design in tools, courses, information communicated and forms of training sessions, with short video clips for greater impact. **Ease of use** of protective tools and measures is an essential part of this.

2.5 Online Media Services

2.5.1 Threat Types

Theft of intellectual property content and **data breaches involving customer account details** are the major threats. Most dangerous are the various attacks that may trap customer details or steal content with **social engineering**. This includes **threats to transactions that may involve financial details** and **man-in the middle attacks**. **Also attacks on local ISPs** (like DDoS that causes lack of availability) are taken seriously, as online media service providers (SPs) may install their own servers within ISPs, with their own logical, but not physical, protection.

2.5.2 Application Areas to Protect

Protection is required for the **content ingest chain** and the **content distribution chain**, for content theft and corruption as well as its **payment transaction services**, against fraud and data theft of customer financial details. This implies protection for several functions:

- **Content distribution network** (**CDN**) – the service delivery platform for online streaming
- **WAN broadband networks** (possibly some mobile in some countries)
- **Content ingest chain** – digital service platform for reception from content providers (CPs)
- **Multiple data centres** – online media service platform, third party cloud hosts, local ISPs
- **Databases** – content and customer details
- **End user devices** – endpoint protection
- Encryption of **data for customer records and payment details**; DRM content encryption
- **Payment transaction applications** at the level of the online retailers.

Media service providers' IT infrastructure is often **cloud-based**. These cloud facilities host large storage volumes for the online content databases (this falls in the cloud storage example described above). Thus, the first level of security protection is from that cloud host provider, for its own cloud infrastructure. Encryption of content plus other security measures for **DRM protection** comprise the next level of protection, which is an SP's responsibility. All content is encrypted end-to-end by the media SP, from ingest from a CP to SVOD (Streaming Video on Demand) download streaming to the customer.

Distribution is via the SP's chosen structure of **CDN**, either in-house, or streaming over commercial CDNs. A mix of internal and external may be employed to feed a distribution chain, which could include **local ISPs** for **local edge caching**. Media SPs may also offer **local storage servers** within an ISP's own data centres (above a threshold peak traffic level). These **caching edge servers** should have NIS protection measures from the online Media SP, as well as physical protection from the ISP.

2.5.3 Solutions

The major priority is to protect the customer base, from any data breaches, as well as the business partners across the value chain – the content providers and the partner ISPs. **Mobile device streaming encryption/decryption** for any mobile device is the way forward. The following solutions are required:

- **Mobile device streaming encryption/decryption** for any mobile device is the way forward.

- **Content encryption** is a major requirement. SPs typically have their own highly efficient solutions for unstructured content.
- **Identification services** are also provided from internal resources. SPs tend to use the infrastructure protection provided by the business partners (e.g. the cloud hosting provider), including **built-in infrastructure security from providers of data centres** and its ISP partners.
- Depending on the SP size, third party managed services may not be used. In such cases, all incidents may be handled internally by the SP's **own security services and response teams**.
- In-house office systems and internal back office systems use third party bought-in NIS products such as **firewalls**, and **anti-malware utilities**, managed internally. On the contrary, a **VPN** may be an outsourced third party element, while email and document systems may also be outsourced (from common providers whose security must be audited). The CDN operations are quite separated from the outsourced business support systems. A key area of current focus is the customer mobile device as streaming may be unprotected.

Generally, future security solutions must be more flexible and heterogeneous, for more diverse media ingest and distribution environments, not just a single closed environment. That will require radical changes to design ideology for security. A common theme in interviews was the **need for better certification of cybersecurity products and services**, coordinated at European level, with EU accredited security certification labs.

Today, many online media services providers either have their own content or are moving into production of their own content. So future global networks must handle content production worldwide, securely. Thus the new products and services in demand for online media service operations will be for global siting of production facilities as well as CDN distribution installations, which cloud services should cover. For instance India and other developing regions that are becoming Internet connected at higher speeds will be the new markets requiring local language content. Original content is already being served in such non-English language markets such as France and Germany but local content production facilities are expected to require far more investment in NIS products and services to protect them.

2.6 Comparison of Needs by Market Segment

A summary of the demands for products and services for the five market segments analysed is shown in Table 4.

Table 4: Preferred Products and Services by Market Segment

MARKET SEGMENT	PRODUCTS	SERVICES
Online banking		
	Database encryption – especially for customer records, with effective key management **Mobile devices - end to end encryption** with customer identity and access management with strong authentication **Standard point product sets** – firewalls, anti-virus, attack alert and identification tools including IDS/IPS products and anti-DDOS tools **Automated remote back-up and recovery** for security purposes (e.g. for ransomware) **Evidential and integrated SIEM** (security information and event management)	**Threat intelligence** **Managed security services** with intrusion detection/protection/recovery services, 24x7 and EFT (Electronic Funds Transfer) surveillance **Audit services** for rating and certification of corporate security levels with gap recognition and banking standards conformance checks **Sector-wide comparison service** for security levels, with ranking **Business recovery services/ SIEM as a service** **Cyber-attack test exercises**

MARKET SEGMENT	PRODUCTS	SERVICES
		Incident sharing service for the whole sector
Online marketplaces		
	Database encryption – especially for customer records, with effective key management **Mobile devices - end to end encryption** with customer identity and access management with strong authentication **Standard point product sets** – firewalls, anti-virus, attack alert and identification tools including IDS/IPS products and anti-DDOS tools **Evidential and integrated SIEM**	**Threat intelligence** **Managed security services** with intrusion detection/protection/recovery services, 24x7 **Cyber-attack test exercises** **SIEM as a service**
Cloud storage		
	Database encryption – for all stored data (especially customer records); key management **Standard point product sets** – firewalls, anti-virus, attack alert and identification tools including IDS/IPS products and anti-DDOS tools **Automated infrastructure configuration management** (OS and application patching) **Evidential and integrated SIEM** **Federated identification and authentication**	**Threat intelligence** **Managed security services** with intrusion detection/protection/recovery services, 24x7 **Life cycle risk analysis** with continuous tests for malfunction with hacking checks and incident reporting, especially data breaches **Cyber-attack test exercises**
Wireless Telecommunications		
	Database encryption – for customer records with effective key management **Automated configuration and patching manager** (possibly using AI) for maintenance of global scale networks – could be an external service **Standard point product sets** – firewalls, anti-virus, attack alert and identification tools including IDS/IPS products and anti-DDOS tools	**Threat intelligence** **Managed security services** with intrusion detection/protection/recovery services, 24x7 **SIEM as a service**
Online media		
	Database encryption – for customer records with effective key management **Content data base encryption** with effective key management **Content anti-theft software** – for DRM and embedded watermarking For **secure multi-screen online distribution** for mobile and other devices (STBs, smart TVs, game consoles, etc.) **Secure Identity and access management** with strong authentication for customer access control, for OTT VOD streaming, audio, etc. Embedded and external smart TV hardware **decoders** and chipsets for conditional access **Standard point product sets** – firewalls, anti-virus, attack alert and identification tools including IDS/IPS products and anti-DDOS tools	**Threat intelligence** **Global managed security services** with intrusion detection/protection/recovery services, 24x7 **Digital forensic investigation/ SIEM as a service** **Evaluation of security level** of firmware, hardware and software **Device penetration testing** **Security training** and outsourced expert staff

2.7 Emerging Trends and Evolution of the Demand Side

In the course of our interview survey with suppliers and users of NIS products and services, we identified six major trends in the European ICT market affecting the security of data, operations, assets and customer trust. Due to their impact on the evolution of the Demand Side for NIS products and services, these trends are briefly presented below and mapped to the corresponding market segments expected to be most impacted by them.

1. **Cloud Services** and the Fragmentation of Enterprise Computing tend to drive a looser architecture than the standard configurations for large organisations of user devices networked into (local) servers and large amounts of (remote) storage behind the servers.
2. The **Internet of Things** is slowly expanding with a growth that is expected to rapidly accelerate introducing vast amounts of devices with underlying technology often from much earlier generations of microprocessor software, firmware and hardware making them quite vulnerable.
3. **Mobile devices** are becoming more prevalent and spearhead the mobile workforce transformation but bring several security flaws in their operating systems, utilities and software and hardware architecture.[25] The service provider business model adds to this with apps downloaded from a store that may not survey them for malware adequately. One further cybersecurity issue is that many sectors have allowed employees to use their own portable devices at work, so "bring your own device" (BYOD) has multiplied.
4. **Software Defined Networks / Network Functions Virtualisation** (SDN / NFV) which are expected to become the norm by shrinking the intelligence in outside plant as the elements are defined by downloadable software to their standard servers and switching cores enabling new network configurations to be formed on demand by SDN flexibility. SDN/NFV has strong cybersecurity implications as it opens new vulnerabilities and requirements for authentication.
5. **Artificial Intelligence and Machine Learning** form the basis for the introduction of Adaptive Applications in different sectors. A development that was often highlighted in our interviews was the expectation of large users and nearly all suppliers of artificial intelligence in applications, especially in NIS measures, both services and products.
6. **Big Data**, i.e. the use of very large data volumes, is becoming increasingly adopted for customer profiling and performance management in many large vertical sectors, such as banking, telecommunications and online retail (and horizontal user groups such as IoT). The major threats lie in customer records, used for profiling and with them personal financial data.

A mapping between these trends and the five market segments examined is given in Table 5.

[25] See for instance, https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines.

Table 5: Impact of Emerging Trends on NIS Products and Services demand in the five market segments

TREND	ONLINE BANKING	ONLINE MARKETPLACES	CLOUD STORAGE	WIRELESS TELECOMMUNICATIONS	ONLINE MEDIA
Cloud	✓	✓	✓		
IoT		✓		✓	
Mobile	✓	✓	✓	✓	✓
SDN/NFV			✓	✓	✓
AI	✓		✓	✓	
Big Data		✓	✓		✓

2.8 Demand Side Criteria for successful Products and Services

It is perhaps useful to try to understand what is a successful NIS product or service in the EU market. We have identified the following characteristics for success, from our interviews and desk research.

Overall, there seems to be a homogeneous approach as to what constitutes a good product or service across the selected market segments, in the sense that no one segment in particular expressed increased preference for any of the standard commercial attributes (technical merits, price / Total Cost of Ownership, pricing model etc.). This is not to say that such attributes are not important but rather that **neither the market segment** (e.g. Online Banking vs. Cloud Storage) **nor the product/service category dimension** (e.g. end point solutions vs. encryption) – or any such combination – **revealed any defining prioritisation in terms of standard characteristics**. Therefore, throughout the interviews in all market segments **there were recurring themes regarding the characteristics of successful products and services**, the most important of which are presented below.

For any NIS offering the key advantage is that it is **demonstrably effective**. We found that all user organisations we spoke to are quite mature enough to investigate claims and determine the effectiveness. **Trust in the supplier** (as mentioned in the preceding section) is a further essential feature.

We start with **services** as that is the growth segment and here being able to demonstrate best practice is mandatory for success, expressed by a range of related features:

- Successful service offerings are **easy to understand, buy and integrate** into the user organisation
- Also, **successful services are end to end**, that is are complete offerings as far as possible so that multiple service providers do not have to be dealt with: **one-stop shopping** is much easier and finger pointing in the event of an incident is less likely
- System integration services, to build the security shield into existing networks, databases and servers is a necessary part of services that is best performed by **the same service provider if possible**
- **Successful services are successfully marketed**, by showing the value of the service to right level of management; that makes cost far less of an issue if the benefits in financial terms can be clearly shown

Product success depends on various attributes, not always considered as the primary features perhaps:

- Ability to be **easily integrated both with other NIS products and supervisory systems and with different subject networks and systems**. They should have **open APIs** for interfacing sensing signals and commands, to and from SIEM management dashboards, for instance.
- A common theme emerged from interviews with NIS suppliers that **verticalisation might not be their best sales strategy**, compared to a general all-industry approach, i.e. successful products in certain globally applicable domains do not generally have segment-specific pertinence.
- **Ease of use, installation and maintenance**. One user noted that learning a new product could take many hours of highly expensive consultants to teach security staff how to use the product – a sum that **far exceeded the cost of the product** and its annual software licences. One user noted that the company **would only purchase products for which it had the in-house skills**.
- A **major market for products is the service sector**. So sales of more sophisticated and high-end products to security services providers who then **offer the product bundled within its services** is another channel for sales. Security operations staff needs products that integrate well with existing products and with existing utilities such as dashboards and databases of incident information with reporting in way that can be integrated easily. They want a minimum of training and efforts on systems integration.
- Products in general are becoming more sophisticated because th**e basic products are increasingly integrated into operating systems, network routers and switches**. The general product trend is to move up the scale in ability for incident detection and response.

3. The Supply Side for NIS Products and Services

Building on the analysis of the Demand Side for NIS products and services based on data collected for the five selected market segments, one overarching theme was that **the NIS market structure overall and the EU NIS market in particular are the dominant factors** in defining the success, or lack thereof, of NIS product and service suppliers.

3.1 The EU NIS Market

3.1.1 The EU NIS Market Characteristics

The EU is a comparatively advanced market in global terms and has been moving into services as the major added value. Small Member States act as a fragmented set currently, but are comparatively sophisticated markets individually. From the EITO[26] surveys, for many companies in Europe, the issue of IT security is becoming increasingly important, so that making improvements in this area is high or very high priority for 2016 for some 63% of Western European companies. Many of the market analyst sources note that the EU market will be driven by increased use of mobile devices, mounting demand for cloud-based security solutions and a trend towards managed security services, rather than products.

Our research shows that **there is no single NIS market in the EU**. Rather, it is a **series of national fragments** that may be grouped into clusters of Member States, largely determined by geography, language, economic and technological development, and perhaps also by the state of advance in cybersecurity. The top-level clusters exhibit national preferences (e.g. in Germany and France). These factors will tend to delay the emergence of a single EU market in NIS products and services and players have learned to live with the differences, and even exploit them. Key characteristics in the EU include:

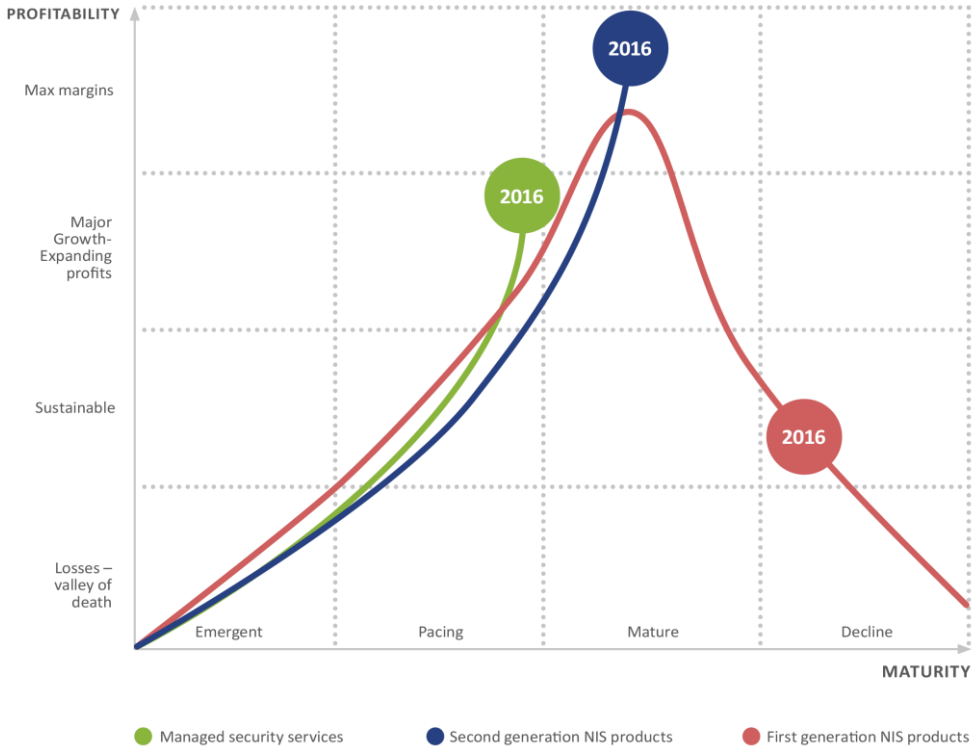
- **The world cybersecurity market is dominated by global suppliers mainly headquartered in the USA**. The enterprise market is largely dominated by global cybersecurity suppliers, again primarily based in the USA. It is important to note, however, that some of these large companies define themselves as multinational rather than American, and may employ significant numbers of people within the EU in a range of functions that go beyond sales, including R&D.
- **Most EU Member States may be defined as advanced cybersecurity markets**, but there are also some less advanced Member State markets. **The EU NIS market is a mature commodity market**, in which most IT hardware and software products are built outside the EU (in Asia and the USA respectively).
- **The market in "commodity" protection products**, close to ICT mass markets (firewalls, antivirus, IDS software, etc.) **is already reaching maturity** and is therefore more costly and complex to enter, while first generation products are stalling in sales.

The NIS market in Europe shows signs of maturity as sales of services rather than products, the coming trend, are increasing. While point products are still important, the move towards holistic solutions means that simpler point products are being replaced by a new generation that may be used in concert with other products that are more sophisticated and "intelligent'. Figure 2 illustrates these trends.

[26] European Information Technology Observatory, Press Releases, 2016.

The EU NIS products and services sector is strongly competitive. A significant growth opportunity for European industry is apparent and this opportunity is widely recognised as more and more advanced businesses increasingly depend on NIS services. The share of services in the EU market has been growing steadily from 41% in 2005 to 47% by 2010.[27] Thus dominance of software and hardware in the EU market has been overtaken in value by services, a sign of its growing maturity. This makes the EU market similar to Japan, where services represented the major share of the market in 2014 (71%), and also to the USA (55%).[28] The software market itself is also undergoing change. Five years ago it was characterised by commoditisation; today we are seeing a shift away from point products such as antivirus software as large software publishers integrate security features into operating systems.

Figure 2: NIS Market Maturity in the EU and the Emergence of Managed Security Services[29]



3.1.2 EU Market Development over the Past Decade

Over the past ten years, threat types and attacks have increased with more attacks being experienced over the past year than ever before.[30] This increase is global, affecting EU enterprises in the same way as firms across the world. Our research indicates that large corporate enterprises typically experience several major attacks per year. Often these may be common DDoS attacks as well as phishing and consumer level endpoint

[27] IDC, 2009, The European Network and Information Security Market: Scenario, Trends and Challenges, A study for the European Commission, DG Information Society and Media, https://www.pvib.nl/download/?id=13029983.
[28] IDC, 2015, Worldwide Network Security Market Shares, 2014: Specialized Products Bolster Traditional Approaches, http://www.idc.com/getdoc.jsp?containerId=259291.
[29] Source: Study analysis.
[30] See ENISA Threat Landscape, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape.

attacks. However, stealthier forms of highly organised spying and business disruption have increased with advanced persistent threats (APTs) type of attacks multiplying.

In response, the need for ICT security has become more important with the media publicly highlighting the growing number of attacks, boosting industry sales, while attack complexity has also increased. In response, since 2010, managed security services have become the dominant segment in the EU, as NIS vendors in the EU and USA have moved in this direction, developing a range of monitoring systems for installed NIS applications, often integrated with alerts and analytics systems as an orchestrated whole. This has been led by major R&D efforts, for example, the advance in artificial intelligence (AI). Such management and monitoring systems are typically at the heart of security operations centres (SOCs) for delivering managed services. Further development of intrusion detection systems (IDS) with threat intelligence and intrusion prevention systems (IPS) counter measures have been added. To cope with the new types of attacks, security information and event management (SIEM) technology has come to fore and consulting to large enterprises also expanded. From our research, the distinction between high-end enterprise solutions and low-end service provider solutions has also disappeared in recent years. This implies that NIS managed services providers with advanced managed services platforms could re-sell via smaller and less advanced services providers; in practice, this means that major providers' solutions that would typically target large enterprise customers can now be resold to small and medium size end customers by smaller local players/resellers who can leverage size, cost base and local presence to provide lower end prices. This is an example of an ecosystem chain forming in the EU.

Currently a major trend is under way in the ICT market itself, with consequent impacts on attack targets. Systems and networks over the past three years have increasingly migrated to virtual environments. Fewer companies are building a complete in-house infrastructure. Infrastructure reduction, however, may vary, ranging from renting rack space in a datacentre to a complete cloud-based application portfolio, including a virtual desktop infrastructure (VDI). So use of public clouds is also rising. Greater emphasis in networking has been placed on software-defined configuration with virtualisation of network functions (SDN/NFV) for telecommunications carriers especially to reduce the cost of infrastructure. The march of virtualisation is continuing, so most NIS vendors now offer virtual appliances for their security modules, aimed at the most popular platforms. Hence the future trend is for highly converged infrastructures in which security, networking and server/storage infrastructure becomes a single managed unit, hosted within a managed remote data centre. This trend also implies that greater protection for shared data centres is a feature of the future EU market as onsite computer centres shift towards remote shared locations.

3.1.3 The current EU NIS Industry Structure

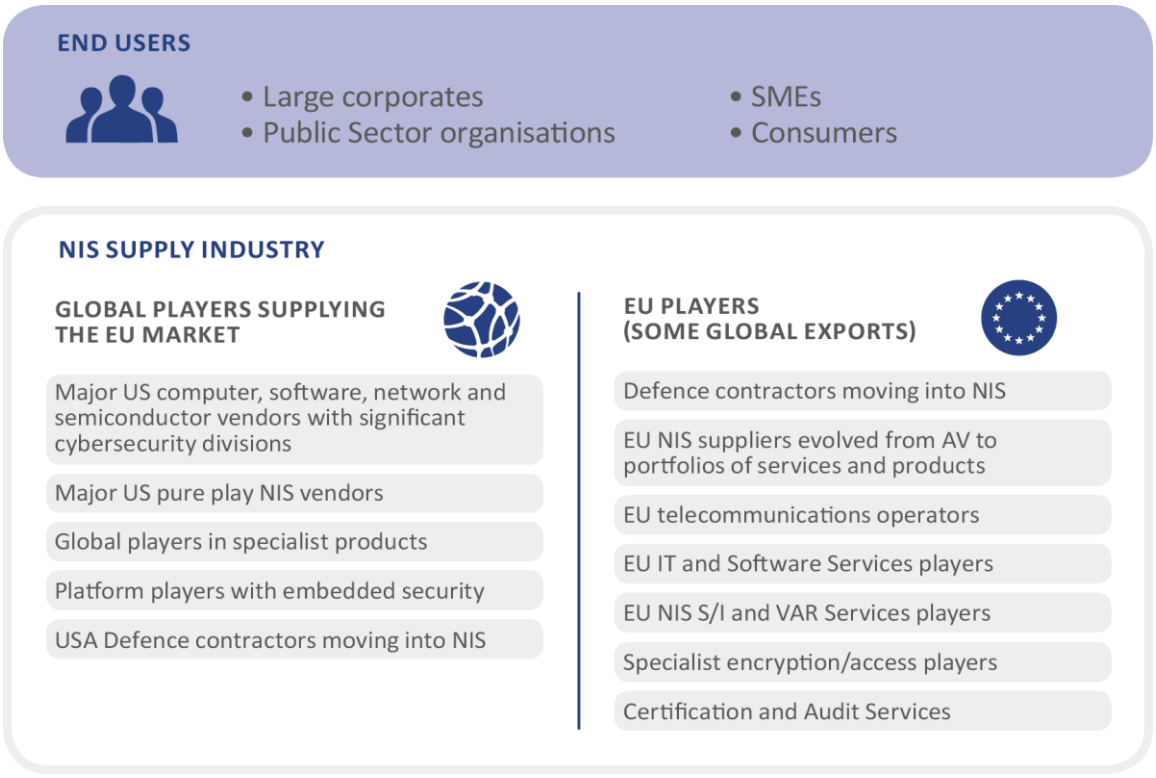
In terms of the NIS industry structure in the EU, typically in most Member States there are only two or three medium-sized NIS suppliers and a large number of much smaller companies. Thus EU NIS suppliers are largely SMEs, who stand alone. **Europe has no large NIS supplier** equivalent to the size of Airbus Industries in aviation. The smaller size of EU vendors makes it difficult to compete internationally especially against the major suppliers, some of whom embed security in their products. To understand the EU supply side, it is necessary to also understand that **while some products and many services originate in the EU, the dominant offerings, in products especially, tend to come from the USA**.[31] Thus today's NIS industry structure in the EU and USA is a mix of OEM suppliers, service providers, system integrators and resellers in a long ecosystem tail of interdependencies:

[31] This analysis was given in various interviews, with Israel also being considered as a major product source.

1. Specialist large and medium NIS software and services suppliers from all over the world, who are often entering the NIS market from the software and computing industries, frequently by serial acquisition of niche NIS vendors.
2. Traditional system integrators with NIS divisions and also small specialist VARs and S/Is who are EU-based and exploit local language requirements.
3. Computer systems suppliers who have moved more into services.
4. Start-ups are key to NIS services and products, especially those in incubators, who reply to the latest threats as they appear; they are often nurtured by the major NIS vendors, who may then absorb them.
5. Large traditional defence companies with specialist divisions for NIS, usually formed from a series of many acquisitions; these appear in the EU as much as in USA.
6. The ecosystems of very small SMEs, often start-ups, and often associated with a series of university labs and incubators, fed by the defence companies or other larger NIS players.

The mix of major players in the EU market from overseas and indigenous players, with the market structure, is shown in Figure 3.

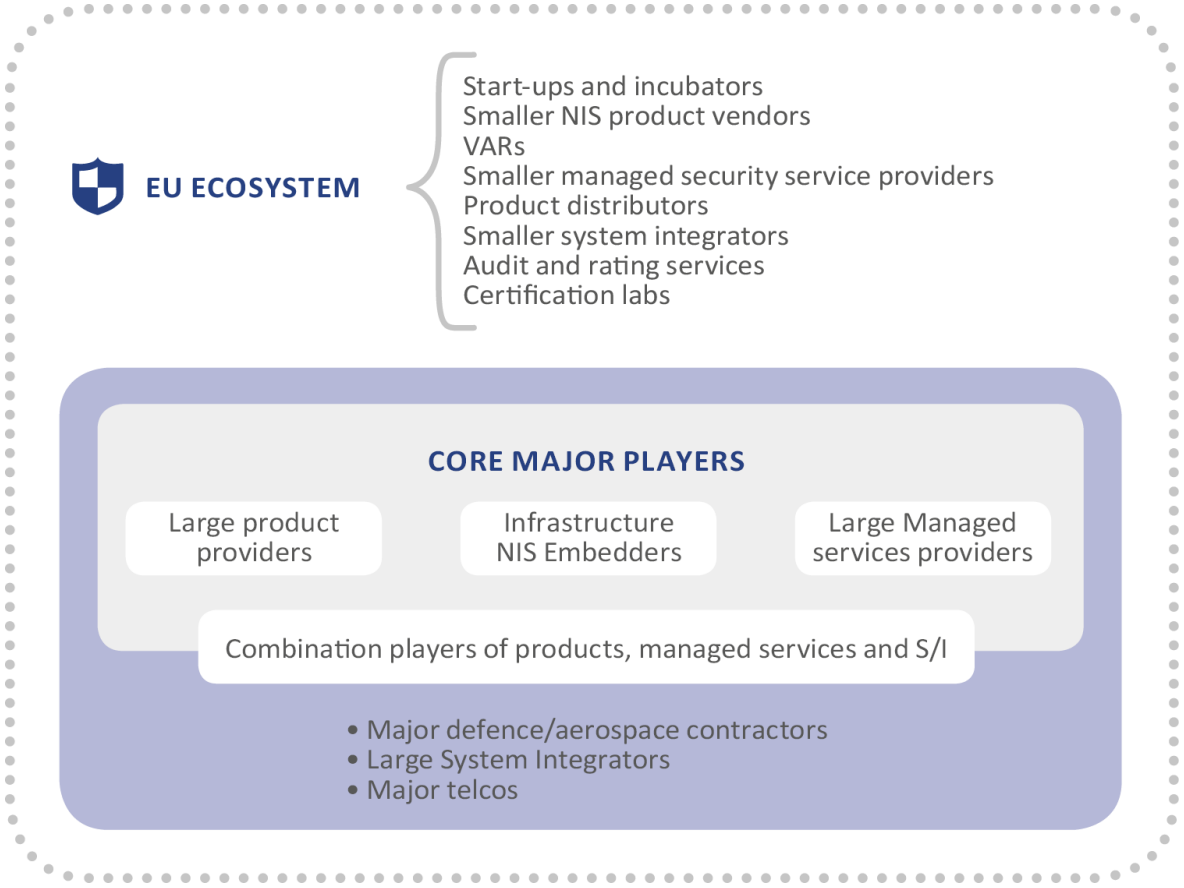
Figure 3: Key Players in the EU NIS Market Structure – Global and EU Categories[32]



Not only are there established specialist global NIS vendors, but also major multinational corporations from adjacent sectors such as ICT, telecommunications, semiconductors and defence who are expanding rapidly into NIS markets. The European market with its ecosystem and dominant major players is shown in Figure 4.

[32] Source: Study research.

Figure 4: The EU Market with its Ecosystem and Core Major Players[33]



Two main approaches to corporate expansion are apparent:

1. **Internal organic growth** through heavy recruitment;
2. **Acquisition of rivals or new segment players**, to gain key technologies and additional skilled headcount.

EU NIS players are equally acquisitive and research among established EU NIS vendors shows a trail of acquisitions.

[33] Source: Study research.

3.2 The Global NIS Market

3.2.1 Characteristics of the Global NIS Market

There is no consensus over the respective figures as the estimates of the total global market size and that of the USA are highly variable, perhaps due to differing definitions of what is included and the rates of growth also differing. One report finds[34]:

- In 2015, the top five vendors together accounted for 37.6% of the security software revenue market share. These vendors also displayed a collective relative decline of market share of 4.2% in 2015, while the rest of the market grew strongly at 9.2% year on year
- Worldwide security *software* revenue totalled $22.1 billion in 2015, a 3.7% increase from 2014.
- SIEM remained the fastest-growing segment in 2015, with 15.8% growth.
- Consumer security software showed the sharpest decline at 5.9% year on year.

Turning to forecasts of spending[35]:

- The largest region for total IT spending in 2016 remains North America, with $1.18 trillion. However, the fastest-growing region is Emerging Asia/Pacific, with 2016 constant-currency growth of 4.8%. The next fastest growth region is the sub-Saharan Africa, with 2016 constant-currency growth of 3.4%. The remaining regions are facing low growth rates - between a negative 0.8% and positive 2.2%. To compare this, the *enterprise software market* is estimated to grow by 7% in 2016 in constant currency. This growth reflects expectations for the office suite market that are driving a five-year CAGR of 7.1%.

Looking at managed security services[36]:

- The Managed Security Services Market is expected to reach US$29.9 billion by 2020 with a CAGR of 15.8%. Security information and event management (SIEM) to be highest revenue generating segment by 2020.

3.2.2 Value and Annual Growth of the Global NIS Market

The value of the global NIS market is the subject of many and diverse analysts' estimates, a selection of which are summarised in Table 6.

Table 6: Estimates of the Value of the Global NIS Market

SOURCE	MARKET SIZE (PRESENT AND FUTURE ESTIMATES)	FUTURE CAGR ESTIMATES	DEFINED MARKET SCOPE
Markets and Markets April 2014	NIS Global: $ 95.6b in 2014 Estimated to grow to $155.74b by 2019	Global CAGR of 10.3% between 2014 and 2019	Scope includes segment breakouts by security type (network, endpoint, application, content, wireless, cloud) and 13 explicit solution type categories.
IDC/McAfee. Centre for Strategic and International Studies June 2014	Global NIS addressable market $58.2b in 2013, up from $53.6b in 2012 Security "Product" portion worth $32.1b in 2013, up from $29.9b in 2012	8.7% growth between 2012 and 2013 NIS Product market running at 14.3%	Bottom-up estimate leveraging several IDC analyst resources containing 17 NIS product/service sub-segments plus estimates from other niche categories.

[34] Gartner (2015) Report on Security Software Market Growth 2015.
[35] Gartner Forecast, IT Spending Worldwide in 2016.
[36] AMR Managed Security Services Market 2013-2020.

SOURCE	MARKET SIZE (PRESENT AND FUTURE ESTIMATES)	FUTURE CAGR ESTIMATES	DEFINED MARKET SCOPE
		growth pa between 2013 and 2014	
Frost and Sullivan February 2014	NIS global market estimated at €62.4b (~$80b) increasing to €111.2b (~$144b) by 2020	Global CAGR of 13.4% estimated between 2014 and 2020	Major cybersecurity applications analysed include network security, data security, endpoint security, and ID and access control.
Gartner August 2014	Global Information Security Spending estimated at $71.1n in 2014, up 8% from 2013. Estimated to reach $76.9b in 2015	8% CAGR estimated between 2013 and 2015	Definition of scope not clear.
Pierre Audoin Consultants 2014	Security IT Services and Software market estimated at €31.5b in 2013	8.5% CAGR estimated between 2013 and 2017	Narrower in scope, focus on NIS services rather than hardware security appliances, so lower estimate expected.

Sources: Various.[37]

3.2.3 Major Cybersecurity Market Segments by Value

Although many analysts produce estimates of the overall NIS market, the scope and definition of the various NIS product/solution categories varies significantly and direct comparison is difficult. Historically, the largest segments under this global analysis include Security Integration Services, Firewalls, Consumer Security Products, e.g. Antivirus and Identity and Access Management (IAM). Segments with the highest growth rates include Forensics, Security Information and Event Management, Vulnerability Assessment and IAM. The increasing fragmentation and diversity of available NIS technologies is reflected in the *Other Categories* segment with a high growth rate. The global market figures for these major segments are summarised in Table 7 for 2012 and 2013.

Table 7: Current Global NIS Solution Sub-segments[38]

NIS SUB-SEGMENT	2012 ($ BILLION)	2013 ($ BILLION)	% SHARE OF PACS MARKET (2013)	YEAR ON YEAR GROWTH (%)
Integration Services	8.1	8.5	14.6	**5.2**
Firewalls (General + Next Gen)	5.4	5.8	9.9	**8.2**
Consumer Security Products	4.6	4.9	8.4	**6.0**
Identity and Access Management (IAM)	4.4	4.9	8.3	**10.0**
Consulting Services	4.4	4.7	8.1	**7.5**

[37] Cybersecurity Market - Global Advancements, Forecasts & Analysis (2014-2019), April 2014, Markets and Markets, http://www.researchandmarkets.com/reports/2820909/cyber-security-market-global-advancements#pos-10; Net Losses: Estimating the Global Cost of Cybercrime, April 2014, McAfee, Centre for Strategic and International Studies, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf; Global Cybersecurity Market Assessment, February 17th 2014, Frost and Sullivan, https://www.marketresearch.com/Frost-Sullivan-v383/Global-Cyber-Security-Assessment-8057049/; Gartner press release, August 2014, http://betanews.com/2014/08/22/information-security-spending-to-grow-8-percent-in-2014/.

[38] Source: Centre for Strategic and International Studies and McAfee (2014) Net Losses: Estimating the Global Cost of Cybercrime, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

NIS SUB-SEGMENT	2012 ($ BILLION)	2013 ($ BILLION)	% SHARE OF PACS MARKET (2013)	YEAR ON YEAR GROWTH (%)
Corporate Endpoint	3.4	3.7	6.3	**7.1**
Email Gateway	2.4	2.6	4.5	**7.2**
Web Filtering	2.0	2.1	3.6	**6.6**
Intrusion Prevention Systems	1.9	1.9	3.3	**2.5**
Security Information and Event Management	1.4	1.6	2.7	**11.2**
Vulnerability Assessment	0.9	1.0	1.7	**10.0**
Policy and Compliance Solutions	0.9	1.0	1.7	**9.9**
VPN	0.7	0.7	1.3	**2.9**
Proactive Endpoint Risk Management	0.5	0.5	0.9	**5.0**
Forensics	0.3	0.4	0.6	**21.0**
Security Device Systems Management	0.2	0.2	0.3	**-7.3**
Other Categories	12.1	13.8	23.7	**14.2**
Total Available Market	53.6	58.3	100.0	**8.7**

3.2.4 Growth Trends of the Global NIS Market

The future global NIS market growth is likely to be fastest in Asia, although all markets (EU, USA, Asia and Rest of World) are growing fast. In China and India as well as Japan, NIS suppliers from the EU and USA are at a disadvantage as their markets are increasingly closed to outside suppliers.

Asian countries outside China and India such as Vietnam, Thailand and others may be growing in demand for EU NIS offerings, as an alternative to those from China. In the poorer Asian countries of Bangladesh, Philippines, Sri Lanka, Pakistan and Myanmar, there is lower demand that is completely price-based. Moreover internal Asian political rivalries tend to dominate – e.g. it is not possible to sell in large volume to both Pakistan and India, or to India and China. The less developed Asian Region countries depend on the degree of ICT infrastructure build and the level of awareness of their governments to invest in NIS protection of the public sector and thus to encourage NIS investment by the private sector. Thus the focus for exports overseas could be on expansion into Asia beyond those named closed countries for the next five years, perhaps, with Latin America and Africa later on.

3.3 Supply Side Analysis – The Emerging Trends

From our interviews and desk research, we have identified the impact of the emerging trends in terms of technology and threats to the evolution of the Supply Side in two dimensions:

1. How the emerging threats and technological trends in the selected market segments will shape the **evolution of the NIS products and services offerings**.
2. How the trends related to future requirements for NIS products and services will shape the **evolution of the EU NIS Market and Industry**.

These two aspects of the Supply Side evolution driven by emerging trends are analysed in the following.

3.3.1 Evolution of NIS Products and Services

The interviews and the desk research revealed that the evolution of the NIS products and services offerings in relation to the selected market segment will be driven by a combination of factors, namely:

1. **IT trends** that will impact the demand for NIS products and services, as described in Section 2.7
2. The **evolution of threats and targets**, as identified for instance in the ENISA Threat Landscape[39]
3. **Future threats against European society** and their impacts, which manifest themselves at a citizen level (identity theft, fraud etc.) and at Member State or corporate level (Critical Infrastructures, Corporate attacks etc.), and that may have an adverse impact in the DSM growth.

In response to the dynamics of the Demand Side driven by these factors, our survey revealed certain directions that the EU industry is taking in terms of developing the NIS products and services offerings.

In such an environment, **identity and privacy will become a key issue**. Authentication solutions have been present in access systems for the past decade but we may expect:

- **Stronger authentication and access control** for almost all applications, especially for those involving any personal data that can be used for tracking and identity theft and financial fraud. Social networking will have to become safer to use.
- **Cloud-based identification and access management** (IAM) providers could produce many new authentication, access and accounting (AAA) solutions. So current authentication mechanisms for access between human users and/or their personal apps or websites or for personal or business related networked applications would tend to reduce, and possibly disappear for some applications.
- **Biometrics** has not fulfilled its promise as a reliable authentication method so far but a new generation using more sophisticated methods might possibly have to emerge from the cloud provider community if they are to flourish, leaving two-factor identification and authentication behind.

As a result of these developments there are cases where the value of the **internal trusted network** comes into question, as against public networks, which should have major protective measures embedded to protect everyone. That should of course be the case also for sectors such as the emergency services for Public Protection and Disaster Relief (PPDR) and health industry applications where efficient protection is vital for safety of life. All of these trends point towards:

- Fewer sales of separate **AV products as they become embedded in infrastructure**
- **Security intelligence plus analytics** are the two key growth areas for the future and they combine **opportunities in services**, perhaps more than in products
- **Changing use of point products** such as firewalls
- Today's levels of authentication are becoming obsolete as more **robust solutions enter and raise the standards of identification**
- **Increased use of encryption** for customer data but with new levels of security as novel processing technologies appear (e.g. quantum computing) as future candidates that may be capable of deciphering current levels of encryption technologies much more easily and quickly.

Additional trends in NIS products and services offerings include the following:

[39] ENISA (2016), Threat landscape 2015, Jan 2016, ETL 2015 -1, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

- The biggest growing threat may actually be the *insider* threat. It may be countered by future services using products that will employ **AI developments for specific situation analytics**.
- Today there are no "**packaged product solutions**" that have the ability to rapidly detect and respond to ransom attacks. For their enterprise audit purposes, some larger and more experienced organisations have built a response based on some form of SIEM product, a major effort. Note this is a gap in the NIS tools market.
- Managed service solutions require that the providers connect into the client's infrastructure, whether it be hosted internally or in the cloud and then access the most critical systems with privileged credentials. **Standardised solutions in order to be able to satisfy internal and external accreditation requirements** will be part of the evolving NIS offerings, particularly when access is performed via the Internet without employing a point-to-point VPN, either IPsec or SSL based.
- SDN tend to concentrate the management and control functions into one or just a few points, increasing vulnerabilities with a single point of failure (or to a small number) rather than distributing the risk across all network elements so **verification and audit capabilities are needed for SDN**.
- A market opportunity exists in **consolidating enterprise security management infrastructure when moving to virtualisation** solutions.
- **Products to protect from financial attacks on mobile financial services** (MFS), including SMS and USSD-type transactions as both mobile banking and mobile shopping are expected to grow.
- **Evolution of security products to productivity appliances**, such as the corporate firewall evolution to productivity control device in managing network traffic, rather than being purely a security device. This is already happening to some extent as often a router operates as a firewall.

3.3.2 Evolution of the NIS Industry

In terms of industry structure, driven by all of these developments, the **managed security services** segment of the NIS industry will become increasingly important.

More generally, the new directions imply expanded opportunities for the EU NIS industry but will **require a stronger R&D element**. As a result, the industry may rapidly restructure to focus on providing and servicing **more sophisticated and easier to use solutions**. That could imply **industry consolidation to ensure R&D funding**. But it will also imply a proliferation of start-ups driven by two forces – the rapid reaction required for responding to new threats and the entry of completely new highly creative ideas.

The banking and financial world already demonstrates the way ahead that the DSM will have to emulate for all types of interactions and transactions. The banks have **guidelines for consumers on how to protect devices**. But those banking service providers cannot make the consumer personally responsible for faulty transactions, or the user population would stop using their eBanking service. That needs to be a general rule applied and enforced across all consumer and business segments of the online market.

To succeed and sustain itself, while driving the DSM, the EU NIS industry may be expected to progressively refocus around:

- A **larger service segment than point products**
- A **structure focused on relationships between vendors**, both EU and headquartered outside. The reality of the NIS market structure will continue to be the strong presence of diverse channels to market for the distribution chain, operated by indigenous EU channel partners in collaboration with vendors that includes system integrators and VARs as well as managed security services providers.
- **Faster threat intelligence and detection** – industry structures for better sharing of threat information and responses with effective cooperation channels and data gathering networks
- More **CSIRTs as a key industry resource**

- **Focus on user protection** in online financial transactions, identity theft and use of mobile devices.

3.4 Characteristics of Successful Suppliers in the EU Market

From our interviews and desk research, we have identified the following characteristics of successful supplier of NIS products and services in the EU market:

- Successful suppliers **operate in many sectors**, not just in a single vertical sector, to spread business risk and address all opportunities.
- They **increasingly offer both services and some products**, or services only as the demand is in that segment while competition in products is fairly intense for the common types.
- They **invest in new technology for greater intelligence or automation**, such as AI based techniques, either by R&D or by acquisition, for internal tools for service provision as much as for products.
- Their **go-to-market strategy (GTM) uses the EU ecosystem** for multiple channels to market, with emphasis on marketing and presence building. The NIS market is one where reputation is useful but real effectiveness is better, as viral marketing via users and suppliers is most important. GTM also requires strong post-sales support with training of users.
- **Privacy is a unique selling point for the EU NIS industry**, which other regions do not have to the same extent. An EU trend that may spread globally is that *ethics are becoming more important*. The EU NIS industry may have an advantage as the USA is perceived as taking privacy and data protection less seriously.
- Successful suppliers **nurture start-ups and incubators** as they will create the new services and products. So leading players seed them, then support them in establishing a steady stream of revenues with early procurement and may acquire them at any stage. This extends to university labs and working with academics as partners in internal team projects.
- They are **able to cope with a fragmented EU market often divided by language and culture**. NIS often requires a specific relationship of trust so customers may mandate that the vendor speak the same language to build this and then conserve it in a long-term relationship. It should result in a transfer from transactional selling to a service-based relationship of repeat sales.
- **NIS business models need to look far more at human centric security**, for instance in retail banking. But this also applies to sophisticated NIS tools to be used by professionals – those that are easy to install, configure and use will succeed over those that need thousands of hours of sophisticated, expensive expertise and hand holding. SOC staff should require the minimum of training for an NIS tool to sell well to the SP segment.
- **Integrate with the rest of the global supply chain** either as a service provider, systems integrator or distributor or product OEM supplier.

4. Strengths and Weaknesses of EU suppliers

Drawing upon interviews with suppliers and users, this chapter examines the strengths, weaknesses, opportunities and threats of the EU NIS market and its suppliers, their commercial and support environment in the EU.

4.1 Strengths of EU NIS Suppliers and the EU Market Environment

The key strengths observed were:

- **Local presence** is important, so local NIS players can supply services where presence is essential for the EU market, for systems integration and local surveillance.
- Successful suppliers are **shifting to services from products**, especially managed services, where locality is key, while products take a lower added value position.
- Security intelligence plus large volume analytics are the **two key growth areas for the future** and they combine opportunities in services, perhaps more than in products. Europe has the expertise for this with some advanced technology, e.g. R&D and centres of excellence in cognitive sciences for AI-based products and services for next-generation of offerings.
- The EU has **industrial competence and manufacturing resources in specialist security technologies** such as chips for SIM cards and credit cards generally, and media encryption for DRM, e.g. for streaming – all of which are applicable more generally.
- **Language skills** for specific Member State markets across the EU helps to build long-term relationships that rely on trust, with language, culture and presence being strong factors in "know your customer" (KYC) for continual services and repeat business.
- The EU NIS market is now strengthening, by **creating larger players** with EU-wide and even global reach from established sister industries, first in system integrators (S/Is) from the existing EU software and services segment, who are now moving rapidly into security and NIS services, especially S/I combined with managed security services. However, note that system integrators are not technology leaders, and so a focus on traditional system integrators as the delivery agents for cybersecurity may be counterproductive. Second, many of the largest telecommunications operators, are entering the NIS services market while making acquisitions to bolster their range in specialised services, product technologies, staff and skillsets.
- Additional strengthening pillars are the **national EU defence contractors**, who are used to working in European consortia. They add a larger scale and are now moving into security with both products and NIS services especially S/I and managed security for the civilian market. Their revenues in the civilian market are mounting faster than the military and PPDR sectors.
- An **ecosystem has formed in the EU market** over the past decade, comprising OEMs, integrators, managed service suppliers, VARs and distributors. This ecosystem thrives from partnerships with overseas NIS product suppliers. Thus EU-based NIS players form the ecosystem for the global suppliers with support for smaller players and offer successful coexistence. The ecosystem of small SMEs, often start-ups, often associated with a series of university labs and incubators, is now being nurtured by major EU players – defence companies, software services players and telecoms operators.
- **Support from the EU, which has expanded greatly** with the DSM initiative, and with the cPPP. Moreover the environment for joint research is fertile with the EU's collaborative H2020 programme embracing all players across the world that are qualified. No similar initiative is available in the USA or China, which extends to overseas NIS suppliers.

4.2 Weaknesses of EU NIS Suppliers and the EU Market Environment

Observed weaknesses emerging from our interviews are principally:

- There is a **fragmented market in the EU**, mainly a set of national markets that lacks the critical mass of the USA or China. Thus the cash flows from "home" market sales limit the ability of EU suppliers to support overseas expansion, marketing and sales forces. The 28 nation state structure also inherently tends to result in corporate fragmentation and the relatively small size of EU NIS players. Thus a large number of NIS companies in the EU are either start-ups or SMEs, with few large companies with global reach. Moreover, larger EU-headquartered players are still emerging in NIS.
- **NIS products and services in the EU have yet to be commonly certified** because of this fragmentation, so any certifications achieved are national rather than Europe-wide and so are invalid outside individual Member States. Public open EU-level standards in NIS are generally lacking and these would help to form a coordinated market.
- EU NIS players tend to **lack EU-wide local presence**, not only outside the EU, but also internally across all Member States. However for services and for some products, local presence may be essential.
- **Most of the underling computing technology used in the EU (servers, operating systems, office systems, databases, mobile device design, web-based systems) originates from the USA**, which tends to put EU firms at a disadvantage when providing security measures for their software and hardware.
- Compared with US firms, EU NIS companies are **relatively poor when it comes to marketing**. They lack marketing communications, account contact and presence compared to their overseas competitors.
- **More R&D financing of EU technical innovation is needed** as well as funding of NIS projects in the developing world, which could use EU NIS products and services. Investing in R&D is expensive for small EU specialist NIS vendors, and participating in EU programmes is difficult. Switching to regional and national levels would need coordination.
- **Limited financing for growth for EU NIS companies** is the norm across the EU, compared to China's state financing with its state owned enterprises (SOEs) and public procurement in the USA and Israel, supplemented by better availability of venture capital funding.
- Some interviewees perceive that there is **too little ambition in the NIS supply industry to really succeed independently**. The aim of small NIS companies is to be acquired, often driven by impatient venture capital investors. Thus they tend not to pursue global success, to expand into "world beaters". This industry condition may be tied to the investment levels of availability and strategic goals of investors, owing to a lack of private venture capital in Europe.
- There is a **considerable lack of training in cybersecurity skills and qualified personnel** that stretches back through to university education in cybersecurity and even further into the introduction of computing and coding, at the level of secondary schools. This impacts awareness in general and is causing a shortage of staff with the qualifications and experience the NIS industry sorely needs.

4.3 Opportunities for EU NIS Suppliers and the Market Environment

Key opportunities exist in:

- Expanding the **next generation of NIS products and services** for more intelligent tools that are sophisticated in both their ease of use as well as in their effectiveness. Then AI could be employed, with massive data mining for analytics from external and internal sources and in real time. This would build on the first generation of NIS tools pioneered in the USA and Israel. However it must be noted that the cost of developing comprehensive AI and analytic solutions is high with large upfront investments. This presents a barrier for the SME and benefits the largest players.
- Over 95% of companies in the EU are SMEs but their needs are rarely catered for in today's NIS industry. The opportunity is a **target market for business customers that are small**, i.e. SMEs and companies

excluding the large corporates. The offering would need to be security as a service (SECaaS) with support designed for the smaller business customer. Naturally one of its major demands, which matches the market generally, would be for tools and user processes that are much easier to configure and maintain, i.e. tools that require less specialised expertise to set up, less training and specialised skills to use.

- There is an opportunity to **develop a service sector** that enables the seamless integration of IT services from multiple sources, allowing organisations to pick, mix and change. System integrators as we know them would disappear and a new breed of service organisation would be the norm with security as a key unique selling point.
- Going further, an opportunity exists to form the EU's SME-level NIS suppliers of products and services into collaborative networks for **stronger EU NIS "wholesale" consortia across the EU** as ecosystems of cross-product bundling with services. System integrators, VARs and larger NIS service operators could act as a reseller channel to market for those SME suppliers too small to have an adequate budget for a sales force or EU-wide marketing. Some of the bigger suppliers are already forming their own clusters and this could be extended.
- Similarly, forming **consortia among large EU defence contractors to produce larger NIS players to address the biggest infrastructure protection challenges**. These EU companies already have decades of experience of working together. They could be joined by the larger players from software and services and telecommunications operators to build EU-wide consortia, on an Airbus or Arianne model of collaborative operation. This would require EU-level encouragement and orchestration.
- **Mobile is the future trend** for most end-users, both business and consumer, to access their systems and services. Consequently, it is a major future growth segment for the cybersecurity business, especially since mobile operating systems are weak in security terms. Closing their vulnerabilities with regular patches is also inadequate, leaving mobile devices vulnerable. That provides a future market opportunity for the NIS industry, especially in the EU.
- **5G small cell technology requires new security considerations**, with its much higher bandwidth into a user business, which may tend to expand the vulnerabilities as large amounts of data can be quickly downloaded, for example if the user loses the handset. Moreover, consumers and business users may have 5G handsets with a Terabyte of data stored within the mobile device and again losing that data could threaten a whole business. This is a new threat area - and a new NIS opportunity.
- **Anticipating the common demands in the IoT market** is probably the single biggest opportunity for the NIS industry. For instance, the IoT's potential use of commercial mobile networks for connection bringing increased exposure to attack is a further NIS opportunity.
- Through **early school education** in secure software development plus development of new professional qualifications at degree and post graduate levels, create a stronger EU-based NIS industry with large numbers of qualified personnel for three areas requiring stronger NIS skills:
    - CSIRT teams to work in SOCs
    - Product development – both NIS and generally, especially for infrastructure
    - Programming of all types – bespoke, embedded, product packages for the commercial market
- **Future global NIS market growth** is also a major opportunity, and likely to be fastest in Asia, although all markets (EU, USA and Asia) are growing rapidly. However, in China and India as well as in Japan, the EU NIS suppliers (and those from the USA) are at a disadvantage as those national markets are closing to outsiders and so are unlikely sources of sales for EU suppliers. Thus the focus for exports overseas could be on expansion into the open markets in Asia for the next five years, perhaps with Latin America and Africa later on.
- New technologies may coincide with **gaps in the market**, often to help the growing segment of managed services providers, some of which include:

- Automated patching tools for very large networks and application configurations including those of cloud service providers, e.g. for global server farms
- AI techniques for threat analysis, e.g. use abnormal behavioural diagnostics to spot anomalies
- AI techniques for intrusion response tools
- Cloud hypervisor protection
- Enhanced encryption, especially key management
- Ransomware response tools for blocking maliciously encryption and/or decrypting such files when attacked

- The EU has an advantage, of a **tradition of consortia across the Member States** that collaborate successfully.
- As a marketing tool to promote EU NIS companies within the EU and internationally, **technical standards for NIS products and services** should be used, such as the German federal agency for cybersecurity, BSI, for ICT approvals but at EU level. An **EU-wide security label** would support European sales. Harmonised qualifications should be created through local national standards but **not as a centralised approach as the EU MS require sovereignty over NIS matters**. Moreover, such standards should be promoted overseas, so EU NIS providers gain global recognition, which is especially significant in the developing world. The standards setting and approvals initiative and its international promotion could be part of ENISA's responsibilities.
- The common perception is that the EU is highly fragmented into 28 states and lacking the USA's single market or its much higher levels of available investments. In reality, some individual Member States lag behind but the collection of advanced EU Member States could lead – some are at the "bleeding edge'. Building the EU NIS industry will require more **focus on opportunity sectors**. E-Government, for instance, should be the first priority and EU governments should set standards for security for that initiative.

4.4 Threats to the EU NIS Suppliers and the Market Environment

Although there are many opportunities for the EU NIS industry, it faces several striking threats:

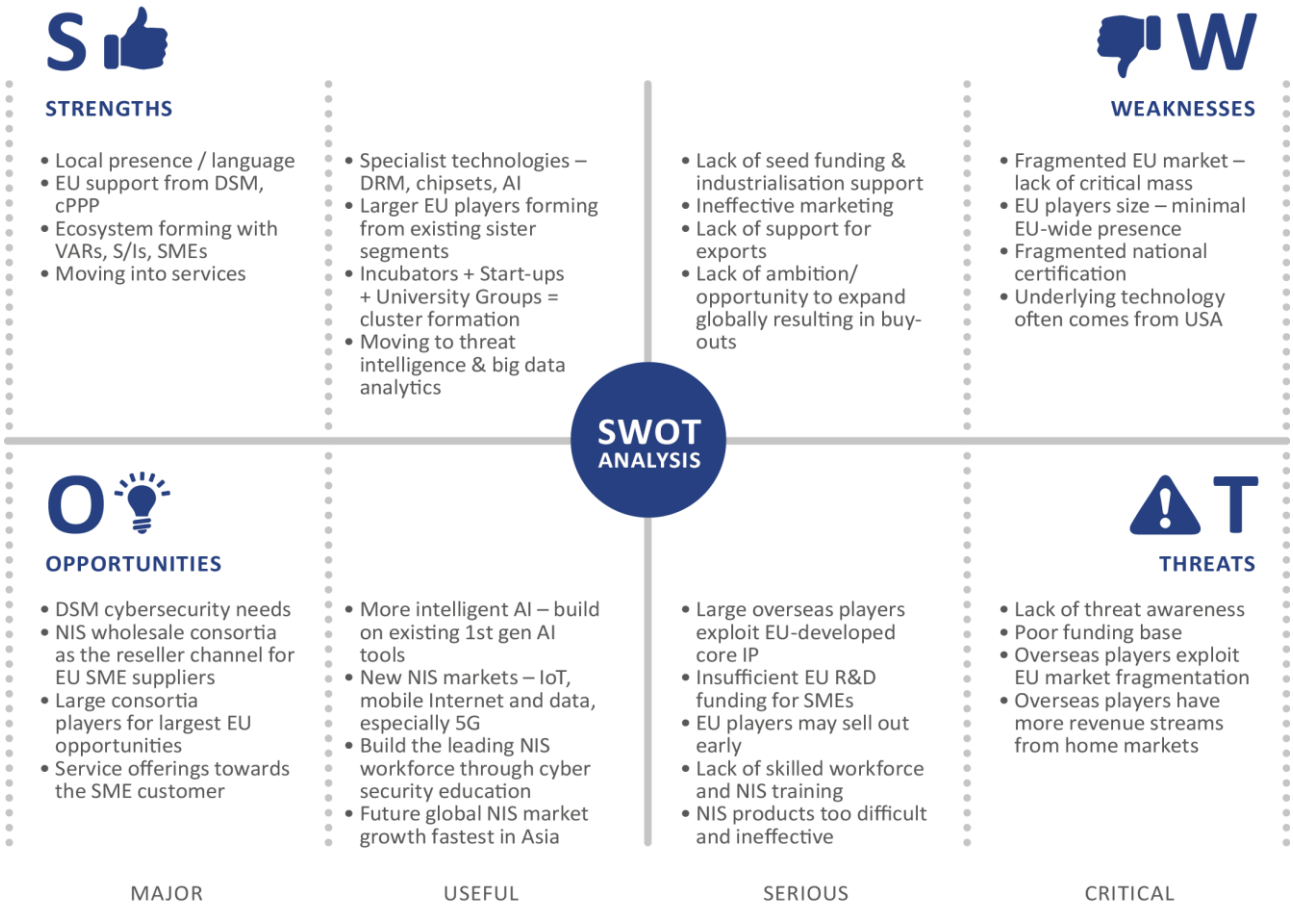
- The major barrier to the EU NIS market growth is the **lack of awareness** of users of the level of threats to business, a common theme across the EU Member States, which is less the case in the USA, which is a more advanced market in general in taking up NIS offerings. This lack of awareness is greatest in the EU's SME segment where governments need to provide more support. Business and the public sector are not being sufficiently educated on the need for security. Major fraud activities touch every level of the population every day, but continued low levels of sales of NIS services and products threaten the EU economy.
- To compound this, **NIS products remain difficult to use** and beyond the reach, in terms of cost and skills required, of the public and SMEs, while large corporations often fail to protect their customers adequately. The result will be stagnant sales unless products and services become more affordable and attractive to use.
- In terms of the global market, the key threat to EU NIS suppliers is that **better funded overseas NIS players** succeed in entirely dominating the EU market. They could exploit the EU's fragmentation by acquiring the best local companies in each Member State, then expanding sales as a common brand across the EU, with major inward investment underpinned by their home markets' revenues (in the USA and China).
- Similarly, it is conceivable that **intellectual property funded and developed in the EU could be bought and exploited by overseas NIS suppliers**, from China and the USA, so that EU investments in R&D may be lost to the EU. In this regard, promising EU suppliers may have little alternative because of the limited EU investment available to enable them to develop the more advanced tools required and bring them

to market. Not only is EU **funding for R&D and commercialisation too limited**, given the scale of AI and large-scale data analytics required, but it is **spread too thinly**, making the creation of a major EU player less likely. Moreover, EU and national funding may be too burdensome to access in terms of costs and bureaucracy for start-ups and SMEs. Thus any promising innovative or existing EU NIS supplier is often acquired by a global player, especially if major equity holders are anxious to realise their investments.

- The **shortfall in the cybersecurity workforce** remains a critical vulnerability for the industry. Conventional education and training policies cannot meet demand. The lack of trained personnel exacerbates an already difficult task of managing cybersecurity risks. Professional certification in NIS is needed to increase the qualified workforce.
- Sometime in the next decade, **new computing technology** could endanger some current encryption technologies. That would open more customer databases to attack for data theft. Confidence in online commerce, and in any business that stores customer or confidential data, could be compromised. Countering this will require further R&D investments in cryptography for new algorithms.

The SWOT analysis is summarised in Figure 5.

Figure 5: SWOT Analysis in Summary



5. Recommendations for Encouraging a Stronger EU NIS market

Given the importance of the DSM to the EU's economy and society, its protection from cyber threats is of crucial importance. This, in turn, demands an **effective European industry to supply the necessary NIS products and services**. This will require an encouraging and supporting initiative at a policy level to go beyond simple R&D support. A **comprehensive cybersecurity industrial policy**, in contrast, would recognise the critical importance of protecting the assets on which the DSM is being built and support not only the research but also its commercialisation.

But there is a dilemma. With cybersecurity being seen as a national competence, achieving an EU-wide response is a sensitive matter. However, the distinction needs to be made that what is suggested here is not EU interference in national cybersecurity but rather industrial policy to support the EU's cybersecurity industry.

Many of the NIS users and suppliers interviewed for this study thought that, although the European Commission has a prime focus on the digital economy, greater emphasis is needed on its protection. To this aim, the following sections makes recommendations for actions that could be undertaken by policy makers at the EU and Member State level. Building an effective European sector for NIS products and services largely depends on the industry itself, and the final section makes recommendations for action from within the NIS industry.

5.1 Recommendations for EU Policy Makers

The European Commission's 2014 Communication, *For a European Industrial Renaissance* stressed the need for Europe to focus on post-financial crisis growth and modernisation and recognised the central importance of industry for creating jobs and growth.[40] The DSM is a response to that and so its protection against cyber attacks is of prime concern. This implies that an industrial policy to encourage and sustain an EU-based NIS sector should also be a principal focus, to provide strategic independence for key areas of the future digital economy in the EU.

The first requirement for an industrial policy to support the EU NIS industry is a strategic vision of its complete scale, operation, risks and key objectives, while the second step would be to understand the various measures that need to be planned and put in place. Collectively, these can be addressed by the following recommendations.

1. **Conduct a needs analysis** with in-depth examination of the objectives of the industrial policy, based on the risks due to technological dependence on ICTs and their consequences for:

    - An EU digital economy, following the DSM concepts, but recognising the global context.
    - The DSM's overall viability in the light of the vulnerabilities to cyber attack
    - Social impacts
    - Sovereignty issues.

2. **Increase awareness of the market**:

    - Promotional planning to educate the market, with professional campaigns in public media for the citizen and for business with promotion of small business and vertical sector information and

[40] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0014&from=EN.

primary training. For larger companies this should focus on accountability and obligations under the GDPR.

- SME policy for small company users to encourage NIS product sales – to improve risk awareness, change attitudes, with some funding of procurement.
- Promote NIS training and educational measures across all levels of education – secondary, university, including computer science, and professional.

3. **Focus R&D planning on supporting the development of innovative ideas and technologies** in the cybersecurity domain and to **strengthen their link to the EU cybersecurity industry**. Here, the Contractual Public Private Partnership on Cybersecurity (cPPP)[41] offers the initial step in industrial support that will be necessary. This will need to be built on with further programmes for industrial level collaborative projects. These should be much easier and cheaper to apply for and more flexible in scope with higher chances of success for SMEs. R&D planning should include support for:

   - Start-ups
   - Incubators
   - Collaborative projects
   - Multiple EU centres of excellence for R&D and training.

4. **Support the industrialisation of new offerings and technologies** following the R&I phase with a public procurement policy of preferential purchases to support SME NIS suppliers moving from innovation to industrialisation:

   - A procurement plan for innovative SME NIS suppliers to offer them early funding of products and services by the public sector and related enterprises, creating first orders for start-ups. Streamlined, faster processes are needed for SME supporting actions, as the public sector rules, especially EU procurement rules, are too burdensome and expensive.
   - Funding for NIS SMEs for industrialising new technology.
   - Support for users who are SMEs to procure services and products from EU providers to support the DSM initiatives, especially sourced from the SME NIS players.
   - Export trade support from EU resources overseas (similar to US support in the EU), e.g. organisation of EU cybersecurity exhibition events.

5. **Support the creation of industrial clusters**:

   - To create clusters of start-ups, SMEs and post-start-up ecosystems, with geographic concentration of resources and cross EU links to smaller players of all kinds, possibly around a university as a centre of NIS excellence, or other permanent institution, such as a testing and certification lab.
   - Clusters could be formed at various locations across the EU.
   - With formation of clusters for vertical sectors also, where appropriate.

6. **Increase the footprint of dedicated NIS operational support centres**, for instance:

   - Vertical sector ISACs for the private sector, integrating public bodies with international threat intelligence

[41] Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research an innovation between the European Union, represented by the Commission, and the stakeholder organisation {C(2016) 4400 final}, https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp.

- A series of centralised EU alert centres (CSIRTs) with participation from the private sector

7. **Promote EU level certification of services/products**. That would engender trust for users within the EU and provide a stamp of approval for international markets that other regions do not have by enabling:

   - Security certification of ICT products and services for software, hardware and firmware, ranging from apps for smartphones to data centre management utilities to real-time industrial control software to chip level security. Certification should be detailed and robust – not just a tick box exercise.
   - Certification of NIS products should be in terms of efficiency, ease of use and effort needed across the product/service lifecycle.
   - Approved centres of certification.
   - EU security branding for certified products and services.
   - Continuous certification processes to track developing products/services.

8. **Enhance the relevant regulatory framework**:

   - Ensure flexibility in the implementation of the regulatory frameworks in a way that promotes and supports innovation.
   - Promote audits of cyber security protection levels in all sizes of company and public sector organizations.

5.2 Recommendations for National Policy Makers

A specific NIS industrial policy will only be feasible if supported by the Member States, EU institutions and agencies, and defined in collaboration with the industry stakeholders. Undoubtedly this will require increased coordination at EU level and may also require legislation.

1. Introduce **public procurement policy of preferential purchases** to support SME NIS suppliers at a National level. It is difficult for SMEs to deal with the public sector today and innovative companies can benefit more from commercial contracts and purchase orders that direct funding.
2. **Foster the creation of innovation clusters** at a National level, bringing together start-ups, SMEs, academia, research centres etc.
3. Draw **national guidelines for cyber protection** for each industrial sector as part of this industrial policy, and such a task would be consistent with an enhanced role for ENISA.
4. Follow a **risk-based approach on national critical infrastructures** and set a mechanism to monitor cyber security readiness levels i.e. as a form of a *national risk register* for critical infrastructure threats.
   - Some Member States already do this (e.g. the UK and some Nordic Member States). Such registers should be updated frequently, possibly in real time, allowing protection measures to be taken.
5. **Promote NIS training and educational measures**:

   - University level qualifications for a new NIS workforce, with a new emphasis on security as a basic computer science
   - Education at school level on the need for cybersecurity in using ICT devices and in writing software
   - Support funds for training NIS service staff for cybersecurity incident response teams, e.g. six-month induction course for several thousand staff annually across the EU, with financial support for training courses and trainees. This would provide NIS service providers of all sizes with a solution to the gap in qualified personnel for the security operations centres (SOCs) that will be a key feature of the future EU NIS industry.

Some of these actions have already been put into motion, For example, the agreed approach of the Commission is already turning to maximise awareness in the cybersecurity community of financing opportunities at European, national and regional level, via existing instruments and channels such as the Enterprise Europe Network[42] and also has initiated the contractual Cybersecurity Public Private Partnership (cPPP) for large-scale funding. Moreover the Commission may complement these efforts with inputs from the European Investment Bank (EIB) and the European Investment Fund (EIF) to accelerate access to finance with further measures.

5.3 Recommendations for the NIS Industry

The EU NIS industry needs to become not just more active, but more pro-active. The key market requirement for the NIS industry is trust. Conversely for consumers it should be made clear which products and services they cannot trust. Standardisation, certification and accreditation are all aimed at achieving trust. The challenge for the NIS industry is how to market this such that it differentiates their products and services from ones that cannot be trusted to the same level. From our interview survey, the following points emerged:

1. The EU NIS Industry should **build on its advantage in the context of Data Privacy and Trust** by focusing on products that cover the GDPR needs, before it starts losing ground to non-EU players.
2. The NIS industry should **explore cyber-insurance as a driver** for stimulating growth in demand and for raising awareness, particularly within SMEs; for instance investment in NIS products and/or acquiring security certification(s) will result in lower cyber-insurance premiums.
3. The NIS industry should **push for standards**, first at EU level, with ETSI being involved, and ultimately for global standards with the IEC and ISO for both services and products.
4. The industry should also **push for harmonised certification across all Member States**, i.e. certification in one Member State would be valid across the EU, and promote EU-level labelling with the certification.
5. On the user company side (Demand Side), **cybersecurity should be a concern at board level of all companies**. To achieve this will require a cybersecurity statement in annual reports for listed organisations. This may require acknowledgement of incidents over the past year and current and future measures that have been put in place to manage risk.
6. The EU NIS Industry should **develop a global mind-set** when setting its goals for growth potential and explore possibilities available outside the EU Market to leverage the global growth in demand for cybersecurity products and services.
7. There is a need to **build the NIS ecosystem**, as the market is moving towards holistic solutions covering the supply chain. Thus industry focus should be on building an ecosystem supporting holistic security solutions. That implies that NIS providers should quickly have a clear view of where they fit into the ecosystem, and promote formation of:
    - SME level clusters around each major player, with incubator support for start-ups.
    - Industry consortia, first from the larger players, and second to form and nurture a healthier SME segment of providers of products and services

[42] *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*. EC COM 410 Final, 05JUL2016,

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu