



Horizon 2020 Program

Dynamic countering of cyber-attacks

SU-ICT-2018



Cyber security 4.0: Protecting the Industrial Internet of Things

D6.2: Market Analysis and preliminary business modelling[†]

Abstract: This deliverable determines the market context of C4IIOT and the relevant business requirements and challenges. Moreover, performs a market analysis using different tools to quantify the size of the market and identify key competitors, market needs and trends, stakeholders and potential customers and users. Finally performs a preliminary business modelling which is the first step to a successful business model for C4IIOT.

Contractual Date of Delivery	30/09/2019
Actual Date of Delivery	30/09/2019
Deliverable Security Class	Public
Editor	<i>Spyridon Vantolas (AEGIS)</i>
Contributors	CRF, IFAG, TSG, HPE, IBM, ITML, STS, VIP
Quality Assurance	<i>Georgia Sakellari (UOG)</i> <i>Sebastien Bardin (CEA)</i>

[†] The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833828.

The *C4IIoT* Consortium

FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS	Coordinator	EL
CENTRO RICERCHЕ FIAT SCPA	Principal Contractor	IT
INFINEON TECHNOLOGIES AG	Principal Contractor	DE
THALES SIX GTS FRANCE SAS	Principal Contractor	FR
HEWLETT PACKARD ITALIANA SRL	Principal Contractor	IT
COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	Principal Contractor	FR
IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD	Principal Contractor	IL
AEGIS IT RESEARCH UG	Principal Contractor	DE
UNIVERSITE PARIS I PANTHEON- SORBONNE	Principal Contractor	FR
INFORMATION TECHNOLOGY FOR MARKET LEADERSHIP	Principal Contractor	EL
SPHYNX TECHNOLOGY SOLUTIONS AG	Principal Contractor	CH
UNIVERSITY OF NOVI SAD FACULTY OF SCIENCES	Principal Contractor	SRB
UNIVERSITY OF GREENWICH	Principal Contractor	UK
VIP MOBILE D.O.O.	Principal Contractor	SRB

Document Revisions & Quality Assurance

Internal Reviewers

1. *Georgia Sakellari, (UOG)*
2. *Sebastien Bardin, (CEA)*

Table of Contents

LIST OF TABLES.....	5
LIST OF FIGURES.....	6
LIST OF ABBREVIATIONS	7
EXECUTIVE SUMMARY	8
1 INTRODUCTION	9
1.1 PURPOSE AND SCOPE	9
1.2 APPROACH FOR WORK PACKAGE AND RELATION TO OTHER WORK PACKAGES AND DELIVERABLES	9
1.3 METHODOLOGY AND STRUCTURE OF THE DELIVERABLE	9
2 IOT MARKET ANALYSIS.....	11
2.1 IOT MARKET OUTLOOK	11
2.2 GLOBAL IOT MARKET SIZE AND GROWTH FORECAST	12
2.3 IOT INDUSTRY CHALLENGES	17
2.4 IOT INDUSTRY OPPORTUNITIES	19
2.5 IIoT MARKET OUTLOOK	20
3 IOT CYBER SECURITY MARKET	23
3.1 MARKET DEFINITION	23
3.2 MARKET SEGMENTATION	23
3.3 IOT SECURITY INDUSTRY OUTLOOK	24
3.4 ECONOMIC TRENDS IN THE EUROPEAN INDUSTRY	29
3.5 MARKET DYNAMICS	31
3.6 STAKEHOLDER ANALYSIS	38
4 COMPETITOR ANALYSIS	41
4.1 INCUMBENTS COMPETITIVE LANDSCAPE.....	41
4.2 IOT STARTUPS COMPETITIVE LANDSCAPE	43
4.3 INDUSTRIAL IOT STARTUPS LANDSCAPE	44
5 IDENTIFYING C4IIOT COMPETITIVE ADVANTAGE	48
5.1 PEST ANALYSIS	48
5.2 SWOT ANALYSIS	52
5.3 UNIQUE SELLING PROPOSITION	53
6 BUSINESS MODEL	54
6.1 BUSINESS MODEL CANVAS	54
6.2 BARRIERS TO ADOPTION / BARRIERS TO ENTRY	58
7 CONCLUSIONS.....	62

List of Tables

Table 1: Factors impacting the market	31
Table 2: Stakeholders' analysis	39
Table 3: Max Fines per Regulation.....	59

List of Figures

Figure 1: Active device connection worldwide	12
Figure 2: Iot Market size	13
Figure 3: IoT Market Share by Sub-Sector	14
Figure 4: IoT Market Forecast.....	14
Figure 5: IoT Spending worldwide	15
Figure 6: Global IoT market	16
Figure 7: Key Factor of IoT Growth.....	17
Figure 8:IoT Security Market	23
Figure 9: Barriers for investments in IoT	24
Figure 10: IoT cybersecurity survey	25
Figure 11: IoT Security Market Size	26
Figure 12: IoT Security Market by Region	26
Figure 13: IoT Security Spending Forecast.....	27
Figure 14: Market Dynamics.....	32
Figure 15: IoT Attack Volume	33
Figure 16: IoT Threats History	34
Figure 17: Classification of stakeholder types with associated strategies for engagement	39
Figure 18: IoT-IIoT Cybersecurity Map	43
Figure 19: IIoT Start-ups.....	45
Figure 20: PEST Analysis	48
Figure 21: SWOT Analysis	53
Figure 22: Business Model Canvas	55

List of Abbreviations

EC	European Commission
WP	Work Package
IOT	Internet of Things
IIOT	Industrial Internet of Things
SWOT	Strengths, Weaknesses, Opportunities, Threats
PEST	Political, Economic, Social, Technological

Executive Summary

This deliverable provides detailed market analysis for the market of Cyber Security in Industrial IoT domain and preliminary business modelling for the C4IIOT framework. The analysis defines the current and expected market and stakeholder requirements to facilitate the establishment of the baseline required for the market projection and the commercialisation of C4IIOT framework.

This report is the first step to a complete business model for the C4IIOT project. The understanding of the potential of IIoT and IIoT security market and the competition landscape will give C4IIOT consortium a way to maintain C4IIOT effectiveness in long term and avert danger.

1 Introduction

1.1 Purpose and Scope

This report presents a market and a stakeholder analysis as well as a preliminary investigation of potential business models that can fully exploit the potentials of C4IIoT. This encompasses the identification of market size and its trends, the key drivers and the regulations, incentives and legal aspects that set the context in which solutions and services for C4IIoT should enter, specifically in the target demos that will be demonstrated during the project. Additionally, it assesses the roles, expectations and benefits for different relevant stakeholders to understand how to leverage and engage them and the main competitors of C4IIoT. The analysis of the current and expected markets and stakeholder requirements and benefits will help the consortium to make future decisions for business plans. This document provides critical information to be able to refine product development and define suitable exploitation strategies for each application and context. Therefore, this report provides a first step in developing the business requirements and business models in C4IIoT project. The understanding of the potential of IoT market, the IoT security market and the competition landscape gives to C4IIoT consortium great insights for the development and exploitation of viable products and services.

1.2 Approach for Work Package and Relation to other Work Packages and Deliverables

This analysis will support the C4iiot implementation and commercialization, by determining the market context of C4IIOT and the relevant business requirements and challenges. Moreover, it will contact a comprehensive market study, using different analytical tools such as PEST and SWOT analyses. This study will quantify the size of the market, identify key competitors, market needs and trends, identify stakeholders, possible clients and users and formulate potential business models to exploit project outcomes. It will also drive both the business and the technical activities of the framework and prepare for the long-term sustainability and potential commercialization uptake to the primary market segments.

The study is a prerequisite for an integrated communication strategy and the adoption of appropriate dissemination and exploitation activities. Based on this analysis we can carve the path to a succeed commercialization and long-term sustainability of the final product.

Combining the results of this study with the results of WP5 (Real-life industrial demonstrations in smart manufacturing) we will be able to match the final product to the market needs and create a strong application that gives solutions to critical cybersecurity issues in the domain of Industrial Internet of Things (IIoT).

1.3 Methodology and Structure of the Deliverable

The methodology employed is mainly based on desk research techniques via literature review, partner knowledge and targeted analysis of domain experts and market research companies.

This deliverable is composed by XX chapters following a top-down approach. Chapter 2 focuses on IoT market in general, presenting the market outlook and highlights the main industry challenges and opportunities that drives the market potentials. IoT will be one of the most compelling technology innovations over the next years and has a direct impact on the main focus of this report, the IoT cybersecurity market that is presented in chapter 3. In particular, in this chapter the definition and the segmentation of the market is presented, highlighting the growth potentials of the market, especially in the European domain, summarizing the main stakeholders and presenting the market drivers, the restrains and the opportunities of IoT cybersecurity market. Chapter 4 focuses on the analysis of competitors in IoT cybersecurity market, identifying their strengths and weaknesses of their offerings. The competitor analysis leads to the identification of C4IIoT competitive advantage that is presented in chapter 5. The PEST and SWOT analysis leads to the understating of C4IIoT services potential for the better positioning in the cybersecurity market. By getting insights of IoT market, IoT cybersecurity market and competitors' landscape we end up to a preliminary investigation regarding the potential business models to follow in chapter 6. Business Model Canvas is the key business tool that drives the support and evaluation of future C4IIoT final business model.

2 IoT Market Analysis

2.1 IoT Market Outlook

The IoT industry is highly fragmented with a large number of small startups entering the market. An interesting trend shaping the industry is the growing interest of many of the larger IT solutions/service providers who view IoT platforms as high margin solutions that will generate a steady revenue stream through cloud-based, subscription revenue models. This has spurred a number of high-value acquisitions in the past three years, for instance, Jasper's acquisition by Cisco in 2016.

The IoT industry is also seeing activities from many global mobile network operators for **connectivity management platforms** as well as IT solution developers for application enablement platforms. The market has benefitted from the combined effects of a strong lineup of new IoT platforms, a marketing push to educate IT decision makers on the scope of their platforms and sustained demand for platforms in the enterprise and consumer applications segment. Hailed as the 'next industrial revolution', IoT will connect **20 billion devices** or 'things' to the existing internet infrastructure by 2020. Sophisticated sensors embedded into everyday objects are already enabling data led decision making for early adopters across industries. IoT has enabled the 'Connected Home' to become a reality, and as a consequence minimized human effort with inventions such as smart refrigerators that can pre-order groceries through eCommerce. Gadgets such as Amazon Echo Dot and Google Nest represent just the first generation of IoT products, with the best of IoT still to come.

In parallel, Industrial IoT (IIoT) is gaining momentum as businesses mesh Big-data and IoT technologies to create major cost and speed efficiencies. IoT enables disparate machines to communicate using data, empowering managers with the capability to predict a fault before it ever occurs. An IoT infrastructure uses wirelessly transmitted data from robots and machine sensors to sense, predict and then alert technicians to conduct preventive maintenance of critical machinery. Operations leaders use IoT to optimize manufacturing processes and reduce risk of incidents. The automotive and transportation industry is already using IoT to increase passenger safety standards by connecting their vehicles with intelligent systems that predict and prevent accidents.

The IoT industry is highly fragmented with a large number of small startups entering the market. An interesting trend shaping the industry is the growing interest of many of the larger IT solutions/service providers who view IoT platforms as high margin solutions that will generate a steady revenue stream through cloud-based, subscription revenue models. This has spurred a number of high-value acquisitions in the past three years, for instance, Jasper's acquisition by Cisco in 2016.

The IoT industry is also seeing activities from many global mobile network operators for **connectivity management platforms** as well as IT solution developers for application enablement platforms. The market has benefitted from the combined effects of a strong lineup of new IoT platforms, a marketing push to educate IT decision makers on the scope of their platforms and sustained demand for platforms in the enterprise and consumer applications segment. Hailed as the 'next industrial revolution', IoT will connect **20 billion devices** or 'things' to the existing internet infrastructure by 2020. Sophisticated sensors embedded into everyday objects are already enabling data led decision making for early adopters across industries. IoT has enabled the 'Connected Home' to become a reality, and as a consequence

minimized human effort with inventions such as smart refrigerators that can pre-order groceries through eCommerce. Gadgets such as Amazon Echo Dot and Google Nest represent just the first generation of IoT products, with the best of IoT still to come.

In parallel, Industrial IoT (IIoT) is gaining momentum as businesses mesh Big-data and IoT technologies to create major cost and speed efficiencies. IoT enables disparate machines to communicate using data, empowering managers with the capability to predict a fault before it ever occurs. An IoT infrastructure uses wirelessly transmitted data from robots and machine sensors to sense, predict and then alert technicians to conduct preventive maintenance of critical machinery. Operations leaders use IoT to optimize manufacturing processes and reduce risk of incidents. The automotive and transportation industry is already using IoT to increase passenger safety standards by connecting their vehicles with intelligent systems that predict and prevent accidents.

2.2 Global IoT Market Size and Growth Forecast

This section summarizes the estimations and forecasts of various researchers, who all agree that IoT security market has great potentials with impressive growth rate. The **number of IoT connections** will increase at a CAGR of 16% from 6 billion in 2015, to **27 billion by 2025**¹. The three countries competing to capture global IoT market share, by 2025 will be the USA (22%) followed by China (19%) and Japan at 6%.

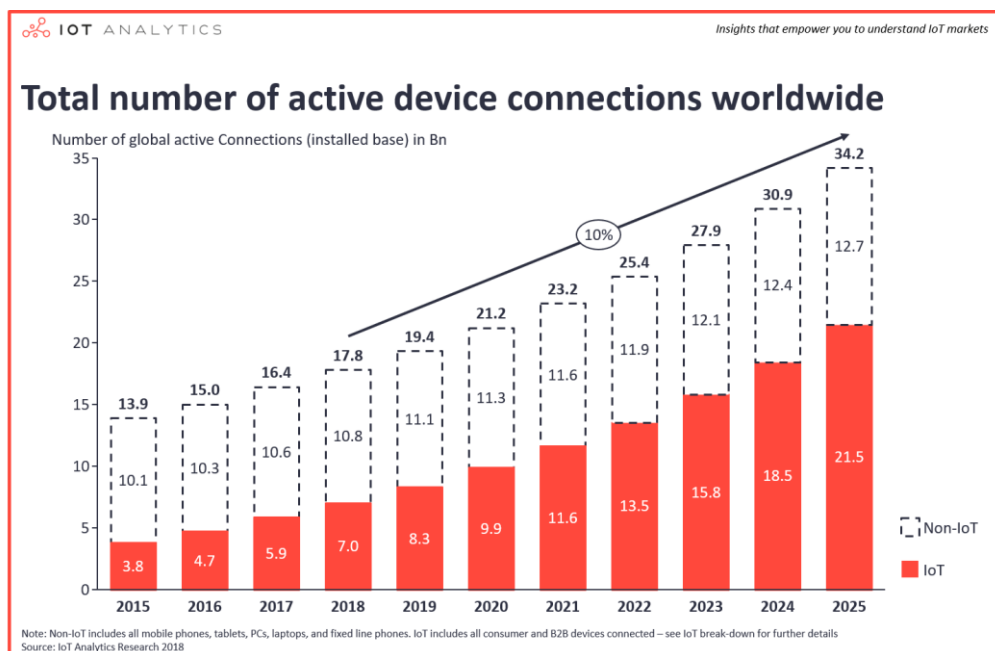


Figure 1: Active device connection worldwide

According to IoT Analytics², latest “State of the IoT & Short-term outlook” update, the number of **connected devices that are in use worldwide exceeds 17 billion**, with the number of **IoT**

¹ Machina Research

² <https://iot-analytics.com/product/state-of-the-iot-2018/>

devices at 7 billion (that number does not include smartphones, tablets, laptops or fixed line phones).

The global connection growth is mainly driven by IoT devices – both on the consumer side (e.g., Smart Home) as well as on the enterprise/B2B side (e.g., connected machinery). The number of **IoT devices that are active** is expected to grow to **10 billion by 2020 and 22 billion by 2025**. This number of IoT devices includes all active connections and does not take into consideration devices that were bought in the past but are not used anymore.

The **global IoT market** will grow from **US \$157bn in 2016 to US \$457bn by 2020**, at a CAGR of 28.5%³.

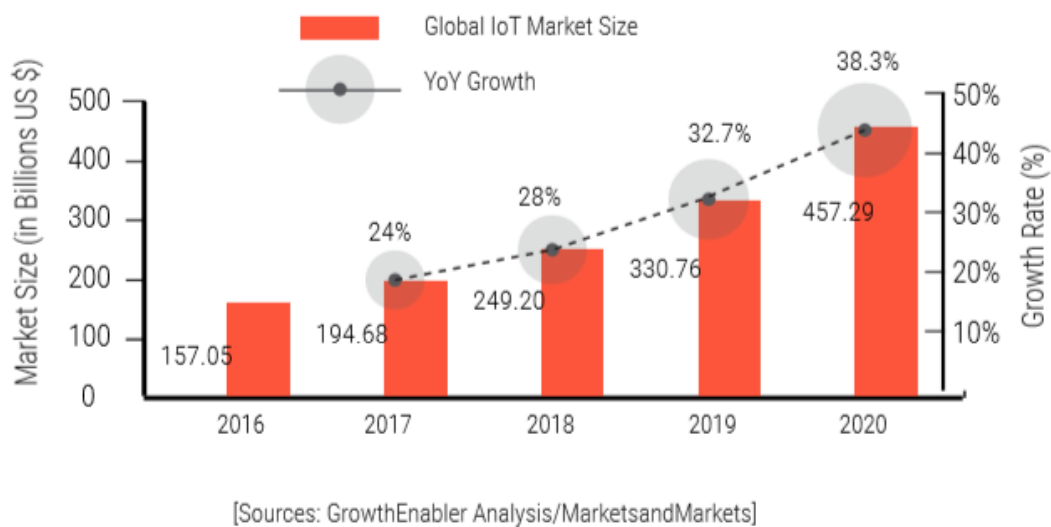


Figure 2: Iot Market size

The global IoT market share will be dominated by three sub-sectors; Smart Cities (26%), Industrial IoT (24%) and Connected Health (20%). Followed by Smart Homes (14%), Connected Cars (7%), Smart Utilities (4%) and Wearables (3%).

³ MarketsandMarkets

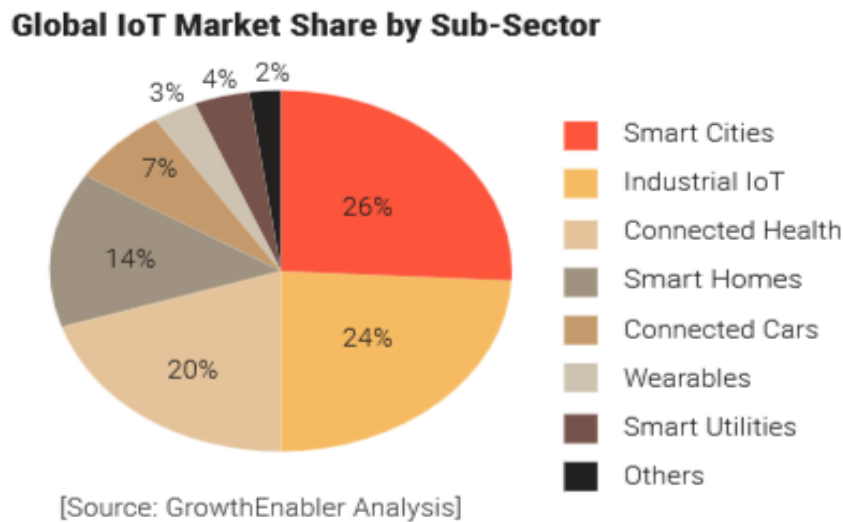


Figure 3: IoT Market Share by Sub-Sector

The global market for Internet of Things (end-user spending on IoT solutions) is expected to grow 37% from 2017 to \$151B. Due to the market acceleration for IoT (as discussed above), those estimates have been revised upwards and it is now expected that the total market will reach \$1,567B by 2025⁴.

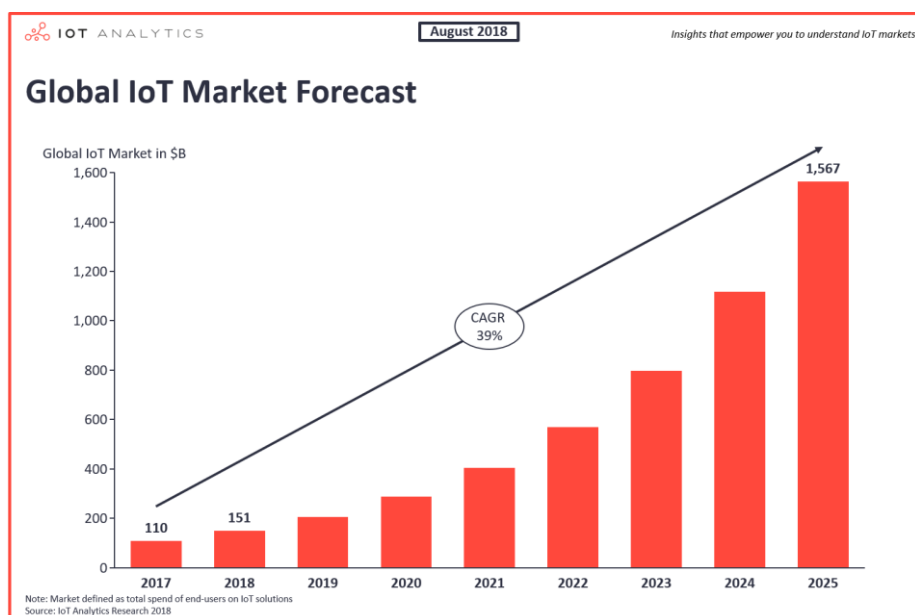


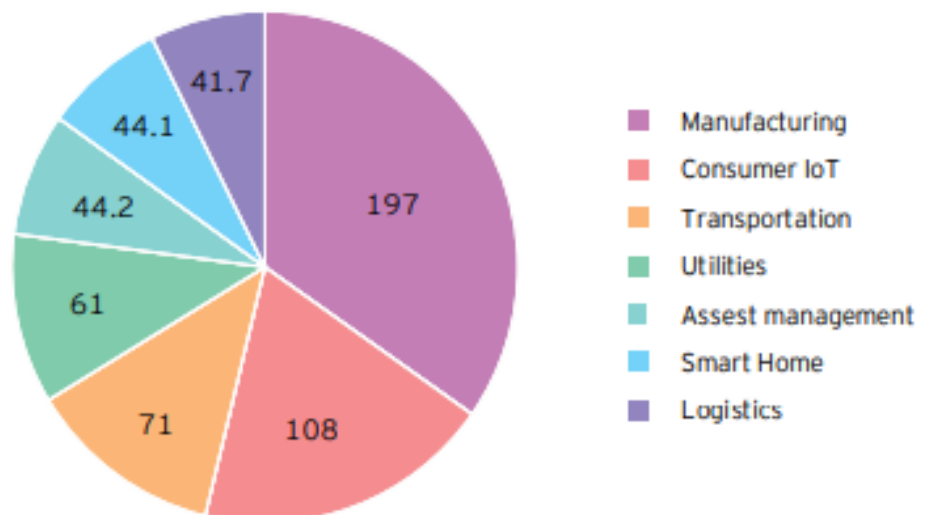
Figure 4: IoT Market Forecast

⁴ <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>

IDC⁵ predicts the **IoT global market revenue** to reach approximately **US\$1.1 trillion by 2025**. Global IoT connections are predicted to increase with 17% CAGR (Compound Annual Growth Rate) from 7 billion to 25 billion approximately from 2017 to 2025.

From a regional perspective, Asia-Pacific region is forecasted to be a leader followed by North America and Europe in terms of IoT market size and revenue with US\$10.9 billion by 2025. Yet **Europe and Middle East (EMEA) is the fastest growing region at a CAGR of 15.7%** through the forecast period. The industries that are forecasted **to spend the most on IoT solutions** in 2019 are **manufacturing** (US\$197 billion), consumer IoT (US\$108 billion), transportation (US\$71 billion), and utilities (US\$61 billion)⁶. IoT spending among manufacturers will be largely focused on solutions that support manufacturing operations and production asset management. In transportation, more than half of IoT spending may go toward freight monitoring, followed by fleet management. IoT spending in the utilities industry may be dominated by smart grids for electricity, gas and water.

IoT spending worldwide (in billions)



Source: EY analysis

Figure 5: IoT Spending worldwide

⁵ <https://www.idc.com/getdoc.jsp?containerId=US44281718>

⁶ EY, Future of IoT

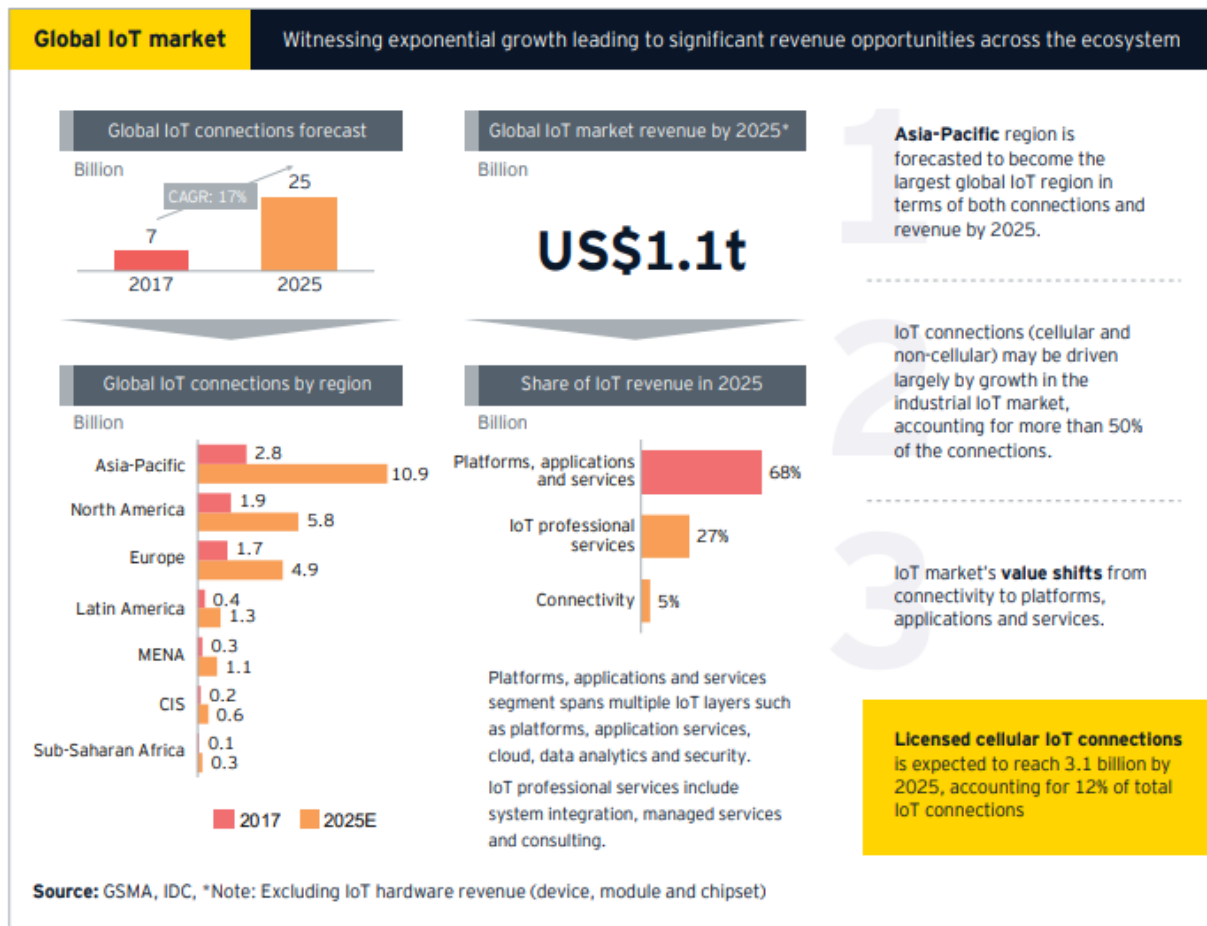


Figure 6: Global IoT market

Global IoT market growth will depend on the following key driving forces in technological, economic and behaviour domain:

- Evolving sensor technology at lower cost
- Rise in high speed networking technologies and higher processing power
- High growth of mobile adoption – connected devices
- Growing adoption and popularity of cloud platforms and cloud computing
- Growing levels of strategic investments to innovate and disrupt/mitigate being disrupted
- Customer demand for improved service and enhanced experience at best cost

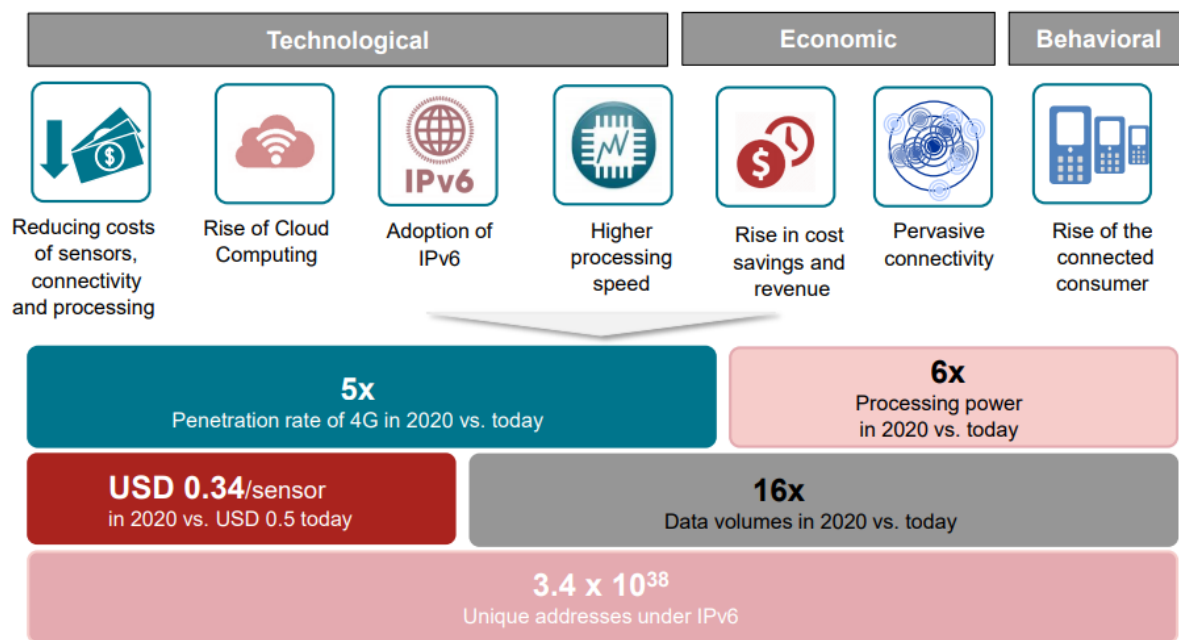


Figure 7: Key Factor of IoT Growth

2.3 IoT Industry Challenges

Every new technology must overcome its fair share of hurdles that often inhibit widespread adoption. IoT is no different. Typical challenges in IoT are not just limited to technical or financial issues, such as the cost of sensor devices, or the investment in network and computing infrastructure, but also relate to intrinsic socio-economic factors.

The progress of IoT is hindered by the complexities associated with governance, security, interoperability, privacy and standardization. Moreover, behavioral and organizational factors such as outdated mindsets, budget constraints, cultural change, day-to-day decision pressures, changing business priorities and the business' appetite for risk - also play a significant role in the widespread adoption of IoT. There is however a way forward for early adopters. Business and technology leaders who invest in research and intelligence and learn by interacting with key IoT experts, investors and startups can identify and pursue exciting opportunities to drive customer experience, optimize costs and grow profits – while outpacing market competitors.

The main industry challenges identified are the following:

Security & Data Privacy

Although the number of privacy laws have increased, the lack of comprehensive data and network security protocols has left every connected IoT device exposed to cyber-attacks, data-breach threats and identity theft vulnerabilities. As an example, Cisco's Talos Intelligence uncovered VPNFilter⁷, a malware campaign targeting router and NAS products affecting

⁷ <https://blog.talosintelligence.com/2018/05/VPNFilter.html>

500.000 compromised devices across 54 countries, with evidence on the first infection dating back to 2016. Similarly, the ‘Slingshot malware’⁸ was discovered by Securelist- a Kaspersky Lab’s division, to be dormant in routers for six years and is capable of information gathering, persistence, and data exfiltration.

Inadequate security of IoT devices and networks is the most pressing challenge faced by the IoT industry as it continues to compound the risk of data vulnerability for both businesses and individual consumers. For instance, in healthcare, any connected patient monitoring system or wearable device can present an open invitation for hackers to steal and share private and confidential information.

High Implementation costs

The global adoption of IoT in a business to business environment is impacted by the high cost of implementation associated with IoT products and solutions. For instance, a manufacturing company with multiple plants, workflows and varying equipment types, seeking to modernize its operational infrastructure, using IoT, will have to consider upgrading legacy infrastructure and systems to achieve a truly standardized and interoperable IoT environment. Policy makers, such as Industrial associations and governments have a significant role to play in addressing this issue by drafting key regulations and standards that reduce costs and drive market adoption.

Adaptability & Interoperability

Interoperability is a core enabler of IoT technology. All IoT devices and platforms need to be highly adaptable and ‘open’ to cater for the widest possible range of applications. For example, if an IoT solution is being implemented in a warehouse to track products, measure inventory and map disparate delivery locations, the biggest challenge will be in making the platform interoperable so that the logistics and warehouse management systems can talk to each other. While progress is being made at standard bodies such as IEEE, Industrial Internet Consortium (IIC) and Open Internet Consortium (OIC), companies in the industrial space are reluctant to bear the cost and business risk associated with replacing existing equipment to accommodate an interoperable IoT world.

Many enterprises are primarily looking for stable yet flexible connectivity stacks that enables them to mix and match sensors, computing infrastructure and analytic platforms based on their needs and business requirement.

Compatibility & Longevity Challenges

Technologies including ZigBee, Z-Wave, Wi-Fi, Bluetooth are currently competing to become the dominant transport mechanism between devices and connectivity hubs. This will result in compatibility issues with the lack of standardized M2M protocols and multiplicity of firmware and operating systems among IoT devices. The sheer number of new standards and initiatives can be confusing and is unnecessarily fragmenting the IoT industry. The IoT industry needs to mature in terms of developing a compatible firmware in their implementation and the standardization of communication technologies.

⁸ <https://securelist.com/apt-slingshot/84312/>

Relative Immaturity & Lack of Clarity for the Industry

Although IoT has been in the market for some time, the adoption of connected device technologies is yet to reach its prime in verticals such as healthcare, manufacturing and other industrial areas. Factors include the additional time required for integration and cost of change; including, upgrading legacy equipment and re-training staff. At this stage of the IoT revolution, there is still a large degree of uncertainty for organizations when considering the total cost structure and revenue potential of their IoT implementations. This has deferred many from making necessary investments in IoT. The confusion created by ever-changing standards has further stalled adoption. For instance, in Healthcare, current implementations in areas such as: patient monitoring, smart medical devices, intelligent hospital rooms, and health wearables e.g. ECG and blood sugar monitors will be key drivers for future market adoption.

In industries leveraging manufacturing automation and clean technology, business models such as smart grids and energy harvesting have been deploying IoT solutions for several years, however many such projects have stalled at the Proof of Concept (POC) stage because the entire industrial ecosystem requires greater market & business model clarity that needs to be validated by early adopters of IoT.

Another major reason why companies are not as quick to implement IoT is because of the scarcity of relevant skills and expertise, according to the World Industrial Automation Survey⁹. As the industry progresses and standards mature, there will be a growing demand for individuals with relevant IoT qualifications, training and implementation skills.

2.4 IoT Industry Opportunities

Continuous advancements in semiconductor technology have reduced the size and price of sensors to the point of its extensive application in connected devices. As consumers, businesses, and even governments recognize the benefit of cost-effectively connecting inert devices to the internet with sensors, IoT's impact and opportunities will continue to grow.

Even if every industry or business sector may substantially vary in the way they leverage IoT, many other sectors including agriculture, power and manufacturing, could start experimenting with small-scale projects that tap into IoT's innumerable benefits like predictive and prescriptive data analytics. Sectors such as advertising and insurance could also take a cue from the consumer utilities, connected cars and healthcare sectors that are at the forefront of IoT investment.

Below we summarize the opportunities of IoT in the industries of interest, namely, manufacturing, logistics and healthcare.

Manufacturing

The primary opportunities for IoT technology in manufacturing industries include predictive maintenance of machinery based on the sensor data collected and production line monitoring with sensors to optimize equipment utilization. IoT implementation would also help

⁹ Morgan & Stanley

manufacturers increase business profitability and productivity of both humans and machines, by streamlining production processes and automating plant machinery with RFID chips that store product configuration data, work instructions & work history.

The copious amounts data collected can also be fed into a predictive analytics engine to make the future manufacturing plants more autonomous in terms of predicting and fixing potential disruptive issues.

Logistics

A great opportunity of IoT technology in logistics industry includes precise inventory tracking and storage management by geo-tagging and geo-tracking assets in real time to achieve efficiencies and speed in order to help improve customer satisfaction and revenue margins. For instance, supply chain and logistics companies can reduce asset losses and moreover, save fuel costs through route optimization. IoT can also enhance predictive maintenance & reduced asset loss by installing wireless sensors inside shipping containers that detect temperature fluctuations and product packaging conditions affecting the usability of perishable food & medicine to reduce asset loss. Also, IoT enabled self-diagnosing devices could identify product issues early, from sensor data to activate predictive maintenance that prevents machine failures.

HealthCare

Research suggests that data-rich analysis of our personal health will become the norm by 2020¹⁰. Furthermore, IoT implementations in healthcare are already enabling quick, safe and real-time diagnosis and treatment of various illnesses. For example, innovations such as capsule endoscopy, being pioneered in the USA by Given Imaging, involve pill shaped micro-cameras travelling through the human digestive tract, while pinpointing sources of illness to improve treatment outcome. The opportunity to leverage IoT innovation to improve clinical effectiveness, drive efficiency and enhance the patient experience across the national healthcare ecosystem is truly sizeable. Examples include, innovations such as hand hygiene monitoring systems, remote health monitoring through wearable devices and smart medical apparatus manufacturing. A combination of smart sensors and cloud computing can also be deployed to optimize the flow of patients, staff, equipment and medical supplies hospital wide.

2.5 IIoT Market outlook

Industrial IoT or IIoT can be explained as the use of internet of things and their technologies in the manufacturing industries to achieve a higher level of efficiency and maximize the quality of products and minimize wastage of resources. Growth in the Cloud Computing and IoT are contributing to the growth of industrial IoT deployments and creating opportunities for new business models of the companies. Various major organizations are planning to practice Industrial IoT to improve the manufacturing process, enhance the business process, business strategy to enhance future business growth.

¹⁰ www2.deloitte.com/content/dam/Deloitte/global/documents/life-sciences-health-care/gx-lshc-healthcare-and-life-sciences-predictions-2020.pdf

The **global IIoT market** is expected to reach approximately **USD 751.3 billion by 2023, registering a CAGR of 23.88%**¹¹ during the forecast period. The market has been divided into various segments based on: component, deployment, connectivity and end-user. By component, the market is segmented into hardware, software and services.

Hardware segment is further segmented into sensors & RFIDs, industrial robotics, camera systems, smart meters, 3D printing, flow and application control devices, distributed control systems and others. The software segment is further classified into MES or manufacturing execution, PLM systems or product lifecycle management system, SCADA system, DMS or distributed management system, retail management software and others. Amongst the hardware, software and services, hardware is expected to dominate the market due to the increasing number of connected devices and increasing application areas of hardware components in the various industrial applications. However, the **software segment** is growing with a fastest **CAGR of 25.65%** during the forecast due to the need of industrial process management and obtaining business insights by processing huge data volumes.

By deployment, the market is classified into on-cloud, on-premise and hybrid deployment. The on-cloud segment is expected to show significant growth due to factors such as easy accessibility to the data or information, easy resource sharing, low operational cost, and growing application areas across various industry verticals. However, the hybrid segment is growing with a fastest **CAGR of 26.26%** during the forecast period, as it delivers combined feature of on-cloud as well as on-premise deployment with additional data or information security capabilities.

By connectivity, the market is classified into wired and wireless connectivity. The wired connectivity segment is expected to show significant growth owing to the need of ownership model and reliable connectivity for data transfer. However, the wireless security market is growing with a higher **CAGR of 26.12%** due to increasing demand of advanced wireless solutions such as Wi-Fi, ZigBee, Bluetooth among others which rapidly boosts the industrial IoT market.

By end-user, the market is classified into IT & telecommunication, manufacturing, healthcare, retail, oil & gas, energy & power, automotive, and others. The manufacturing segment is expected to show significant growth with a fastest **CAGR of 27.94%** during the forecast period as it is the largest consumer of industrial IoT solutions. Introduction of smart manufacturing & industry 4.0 is further helping the market growth.

Geographically, Asia-Pacific is dominating the global industrial IoT market. It is also the fastest growing market, accounting for 38.63% of the overall market share. Significant contribution is witnessed from China, Japan, South Korea and Australia. High presence of industries and increasing adoption of heavy automation and industrialization to connect various industrial processes with the internet are the factors driving the market growth in the region. North America is following Asia-Pacific in the industrial IoT market. Growth in IoT technology and

¹¹ <https://www.kennethresearch.com/sample-request-10077664>

high adoption of cloud computing for industrial processes in the US and Canada is driving the market growth in the region.

3 IoT Cyber Security Market

3.1 Market Definition

IoT can be defined as an interconnected system in which devices are connected using network communication technologies. The IoT security market includes **solutions and services** that are provided to secure the network of connected devices and minimize the losses caused due to threats and cyber-attacks on connected devices.

Despite IoT having a significant opportunity to scale and gain mass market adoption, the **lack of network security capabilities could hamper momentum**. As the number of IoT devices and sensors increase, the importance of data and network security increases too.

3.2 Market Segmentation

IoT security is the latest product category to emerge in cybersecurity. Even though this is a relatively new segment of the security market, it has already diversified and includes multiple vendors.



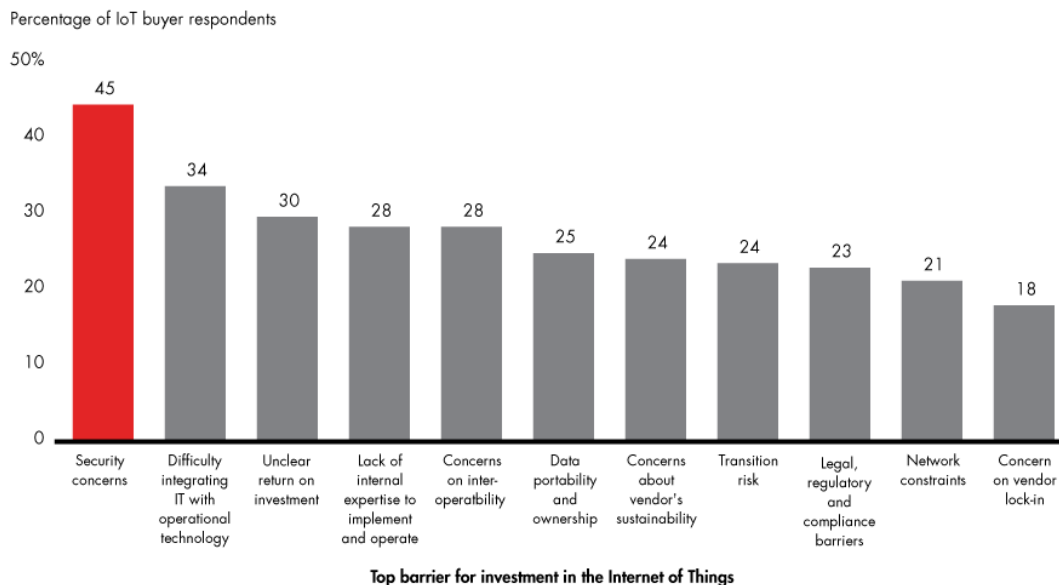
Figure 8:IoT Security Market

An indicative segmentation of the market is depicted below¹², adopting different perspectives of the market and can be analyzed by type, solution, application area, service, component and region.

3.3 IoT Security Industry Outlook

The Internet of Things continues to grow rapidly but concerns about security remain a significant barrier and are hindering the adoption of IoT devices.

■ Security remains the leading barrier for IoT adoption



Source: Bain 2018 IoT customer survey (n=521)

Figure 9: Barriers for investments in IoT

In fact, research by Bain & Company¹³ finds that enterprise customers would be willing to buy more IoT devices if their concerns about cybersecurity risks were addressed—on average, at least 70% more than what they might buy if their concerns remain unresolved.

¹² MarketsAndMarkets, IoT Security Market, Global Forecast to 2023, <https://www.marketsandmarkets.com/Market-Reports/iot-security-market-67064836.html>

¹³ Bain & Company, <https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things/>

■ Customers would pay more and buy more devices if security was better

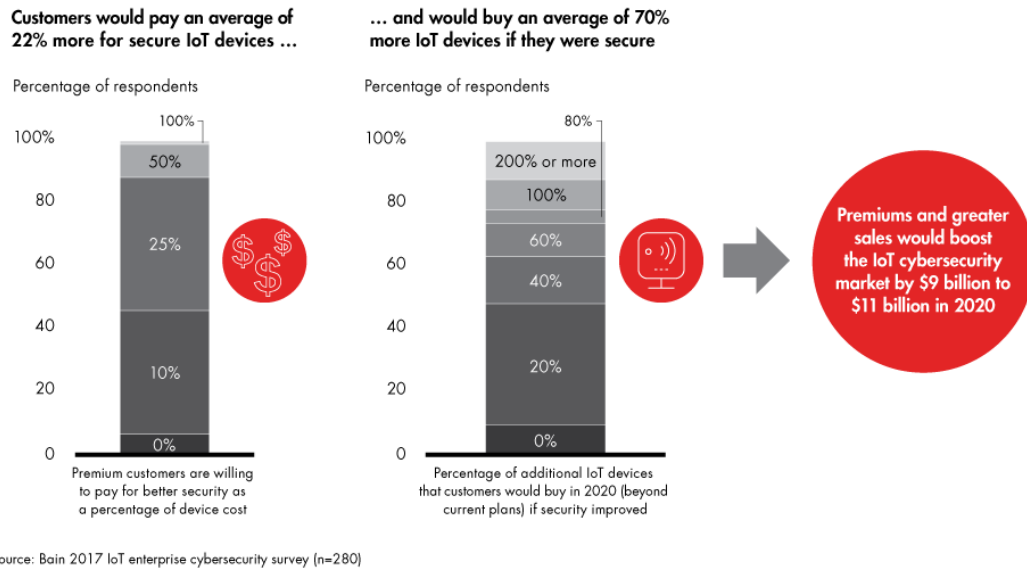


Figure 10: IoT cybersecurity survey

In addition, 93% of the executives, in the same Bain & Company's research, said they would pay an average of 22% more for devices with better security. Taken together, Bain estimates that improving security solutions for these devices could grow the IoT cybersecurity market by \$9 billion to \$11 billion. One reason for this willingness may be increased pressure from new regulations such as the EU General Data Protection Regulation, which imposes strict data protection requirements and penalties on companies for security failures, including data breaches.

The **global IoT security market** size is expected to reach **USD 9.88 billion by 2025**, according to Grand View Research, Inc¹⁴, progressing at a **CAGR of 29.7%** during the forecast period. Surging demand for enhanced privacy is driving the market. Increasing government efforts to implement stringent regulations to restrict the amount of data collected by IoT devices by industries such as BFSI, retail, and healthcare is expected to stimulate the growth of the market.

¹⁴ <https://www.grandviewresearch.com/industry-analysis/internet-of-things-iot-security-market>

A more optimistic forecast regarding **Global IoT security market** is provided by TechSciResearch¹⁵, that estimates IoT security market stood at \$5.67 billion in 2016, and is projected to grow at a **CAGR of 35% during 2017-2022**, to reach **\$31.93 billion**, on account of increasing number of connected devices in the Internet of Things (IoT) landscape and growing awareness among governments and enterprises regarding cyberattacks. Surging adoption of IoT security solutions in the IoT industry, which includes smart homes & connected devices, smart city & business, smart vehicles, etc., is projected to boost demand for IoT security, globally through 2022.

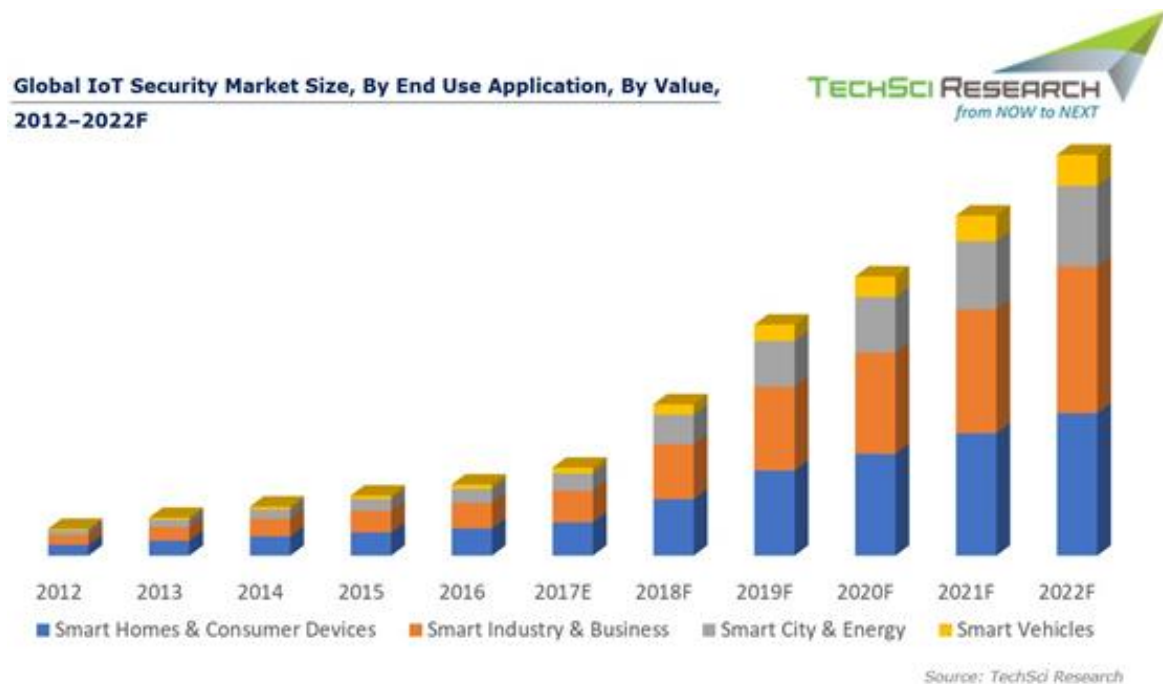


Figure 11: IoT Security Market Size

On the same page, Maximize Market Research¹⁶ values **Global IoT Security Market US\$ 7.8 Billion in 2017** and is expected to reach **US\$ 42 Billion by 2026**, at CAGR of 20.57 % during forecast period with the following breakdown regarding regions:

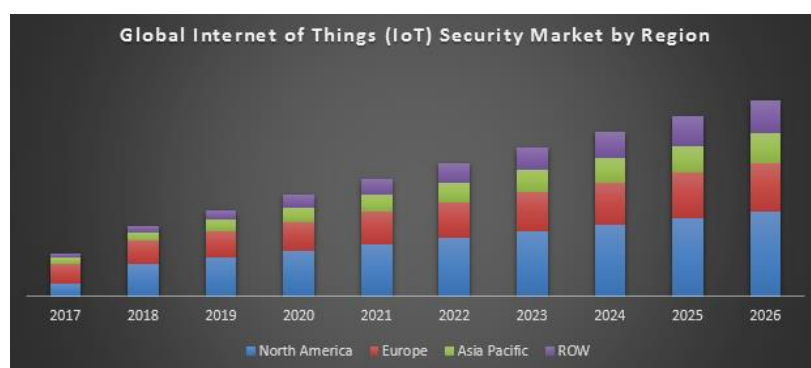


Figure 12: IoT Security Market by Region

¹⁵ <https://www.techsciresearch.com/report/iot-security-market/1509.html>

¹⁶ Maximize Market Research, <https://www.maximizemarketresearch.com/market-report/global-iot-security-market/1543/>

IoT Security Spending

Another insightful aspect of the market potentials is the security spending that companies across the globe are willing to invest in IoT security. According to Gartner¹⁷, nearly 20% of organizations have experienced at least one IoT-based attack in the past three years. The research firm forecasts organizations will increase investments in IoT security to protect their networks and infrastructure.

In 2018 alone, spending on IoT security is expected to increase by 28% from 2017 levels, to reach \$1.5 billion and \$3.1 billion in 2021.

Worldwide IoT Security Spending Forecast (Millions of Dollars)

	2016	2017	2018	2019	2020	2021
Endpoint Security	240	302	373	459	541	631
Gateway Security	102	138	186	251	327	415
Professional Services	570	734	946	1,221	1,589	2,071
Total	912	1,174	1,506	1,931	2,457	3,118

Source: Gartner (March 2018)

Figure 13: IoT Security Spending Forecast

In IoT initiatives, organizations often do not have control over the source and nature of the software and hardware being utilized by smart connected devices. Gartner expects to see demand for tools and services aimed at improving discovery and asset management, software and hardware security assessment, and penetration testing. In addition, organizations will look to increase their understanding of the implications of externalizing network connectivity.

The **professional services sector** is expected to record the highest investment with \$2 billion forecasted to be spent by 2021 followed by **endpoint security** (\$631 million) and **gateway security** (\$415 million). Interest is growing in improving automation in operational processes through the deployment of intelligent connected devices, such as sensors, robots and remote connectivity, often through cloud-based services.

Some key insights of market potentials based on Grand View Research¹⁸ are summarized below:

¹⁷ <https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018>

¹⁸ Grand View Research, <https://www.grandviewresearch.com/industry-analysis/internet-of-things-iot-security-market>

- The **identity & access management** solution segment was valued at USD 255.8 million in 2017, registering a healthy CAGR over the forecast period
- The **professional service** is expected to retain its dominance in the market through 2025 and is projected to reach USD 2.11 billion
- The **application security type** is anticipated to register the highest CAGR of 33.5% over the forecast period
- The **smart home & consumer application segment** dominated the market in 2017 and is projected to reach USD 2.93 billion by 2025
- North America was valued at USD 442.4 million in 2017. It is expected to maintain dominance in the market until 2025. The region was followed by Europe, which accounted for a revenue share of 27.4% in 2017
- Asia Pacific is anticipated to witness the highest CAGR of 34.6% over the forecast period

Industrial Internet of Things (IIoT) or Industry 4.0, is already impacting security in industry sectors deploying operational technology (OT), such as energy, oil and gas, transportation, and manufacturing. Another key factor is the Regulatory Compliance that will drive an increase in IoT security adoption by 2021.

Despite year over year growth in global IoT security spending, Gartner says **lack of prioritization** and implementation of IoT security best practices have hindered the market over the past years. Gartner predicts this **will hinder potential spend on IoT security by 80% over the next few years**. Gartner conclude that while basic security patterns have been revealed in many vertical projects, they have not yet been codified into policy or design templates to allow for consistent reuse. As a result, technical standards for specific IoT security components in the industry are only now starting to be addressed across established IT security standards bodies, consortium organizations and vendor alliances.

Safeguarding future of internet connected devices by robustly configuring necessary/next-generation security features and increasing transparency as well as providing consumers with a choice to opt-out of data collection are some of the key factors driving the market of IoT security.

Increasing use of 3G and 4G long-term evolution (LTE) as well as wireless networks and technologies is augmenting the risk of cyber-attacks. Real-time information and transaction-related information, which are crucial to users, is exchanged through these cellular networks; thereby, giving rise to the need for IoT security. Currently, implementation of the internet is rising exponentially in areas such as health monitors, smart home appliances, smart city projects, and smart retails, which has created the necessity for IoT security.

Adoption of cloud technologies by various organizations for storing confidential data gives rise to risk of unauthorized access to data. Moreover, growing trend of **bring your own device (BYOD)** is increasing concerns regarding data security. Therefore, several organizations and enterprises demand effective security solutions. Thus, a robust security solution, such as integration of firewalls and data loss prevention with IoT security solutions, strengthens organization posture to face cyber threats.

However, **lack of awareness** about benefits and availability of IoT security solution is hampering the growth of the market. **High cost of installation** is also a stumbling stone in the growth of the market. **Lack of expertise** in technical handling, cling to **regulatory compliance**, and **low budget** for implementing new strategies are also some of the factors inhibiting the growth of the market.

3.4 Economic trends in the European industry

Europe has taken a profitable step in adding value to IoT security market, wherein the USD 1.643 billion market of 2015 is projected to reach **USD 6.913 billion by 2020**, at a **CAGR of 33.29%**¹⁹. Germany held a lion share of 31.44% in 2015, followed by France (22.61%).

In the U.K., Transport for London (TFL) has started experimenting different avenues with IoT devices to enhance public services. Similarly, London City Airport is testing IoT applications to enhance customer experience and passenger stream by furnishing customers with more precise doorstep-to-destination information. Nations have begun establishing laws to shield their data from cyber-attacks, which are a goldmine for hackers. The U.K. government declared a five-year, GBP 1.9 billion digital investment plan, along with strategies from government bodies such as GCHQ's Cyber Invest and Government Digital Services. These will handle current skill deficiencies, business coherence management, encryption and fixed security of frameworks.

European Market Dynamics

According to a PWC survey²⁰, 80% of European companies experienced at least one Cybersecurity incident in 2016 and 80% of Europeans believe that the risk of becoming a victim of cybercrime is increasing. Sectors like transport, energy, health and finance have become increasingly dependent on network and information systems to run their core businesses. In the same pace, Europe had more than 200 incidents of theft in 2015 affecting 60 million records. The U.K. had the highest number of breaches, with more than 140 incidents affecting 20.7 million records. Germany came in second place with 11 breaches. Despite the growing threat, awareness and knowledge of cybersecurity issues is still insufficient.



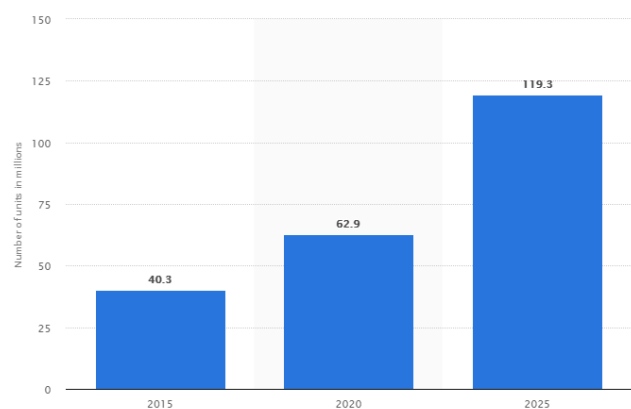
¹⁹ <https://www.mordorintelligence.com/industry-reports/europe-internet-of-things-iot-security-market>

²⁰ PWC, Global State of Information Security Survey, 2016 and <http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/>.

The European Commission has recently announced their next five-year plan in creating digital single market costing over USD 136 billion. The strategy is to pool in all the resources in technology like IoT, 5G and quantum computing to create a huge thrust in the cloud storage infrastructure. Automotive security has been a critical concern for the OEMs and their customers throughout the world. With the market of connected vehicles expected to reach more than 300 million by 2018, driven by the regulation related to safety; the market for cyber security is expected to increase accordingly. Intrusion Prevention Systems (IPS) is one of the major advancements for IoT security incorporated OEMs, Tier 1s, and aftermarket providers.

An essential indication of market potential is the number of **Internet of Things (IoT) units in security** in the European Union and the forecast for the following years.

This statistic²¹ shows the number of Internet of Things (IoT) security units in the European Union (EU) in 2017, 2020 and 2025 (in million). The number of IoT units in the security industry was expected to increase through the years. It was at 40.3 million units in 2017, and it was expected that it would reach **119.3 million units by 2025**. Since the security industry relies on a lot of automation of processes, utilizing IoT devices would be a huge step forward.



© Statista 2019

EU resilience to cyber-attacks

The EU needs more robust and effective structures to ensure strong cyber resilience, promote cybersecurity and to respond to cyber-attacks aimed at the Member States and at the EU's own institutions, agencies and bodies. It also needs strong cybersecurity for its Single Market, major advances in the EU's technological capability and a broader understanding of everybody's role in countering cyber threats. In response, new initiatives to further improve EU cyber resilience and response in three key areas are suggested

- Building EU resilience to cyber-attacks and stepping up the EU's cybersecurity capacity
- Creating an effective criminal law response
- Strengthening global stability through international cooperation

The Commission and the High Representative²² are therefore proposing to reinforce the EU's resilience, deterrence and response to cyber-attacks by:

- Establishing a stronger European Union Cybersecurity Agency built on the Agency for Network and Information Security (ENISA), to assist Member States in dealing with cyber-attacks.

²¹ <https://www.statista.com/statistics/691875/security-iot-units-in-the-eu/>

²² European Commission, State of The Union 2017, Cybersecurity

- Creating an EU-wide cybersecurity certification scheme that will increase the cybersecurity of products and services in the digital world.
- A Blueprint for how to respond quickly, operationally and in unison when a large-scale cyber-attack strikes.
- A network of competence centers in the Member States and a European Cybersecurity Research and Competence Centre that will help develop and roll out the tools and technology needed to keep up with an ever-changing threat and make sure our defence is as strong as possible.
- A new Directive on the combatting of fraud and counterfeiting of non-cash means of payment to provide for a more efficient criminal law response to cyber-crime.
- A Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and measures to strengthen international cooperation on cybersecurity, including deepening of the cooperation between the EU and NATO.
- The EU aims at driving high-end skills development for civilian and military professionals through providing solutions for national efforts and the set-up of a cyber defense training and education platform.

3.5 Market Dynamics

Factors that have a direct or indirect impact on the market are identified and presented in the following table.

Table 1: Factors impacting the market

Factor	Inference
Recent Developments	Recent developments by the top vendors during the last 3 years: The market is fragmented and recent developments are high so it has direct impact on the growth of the market.
Regulations	There are many regulations, which exists but does not have direct impact on the IoT security market
IoT Spending	IoT spending is high in various industries located in several regions. Hence, the high adoption of IoT applications across industries is expected to drive the growth of the IoT security market.
Technology Maturity	IoT security is in the maturity phase.
Government Initiatives	Government initiatives and projects have a direct impact on the market. Initiatives taken by governments across the globe are more in-line with IoT security

Start-up ecosystem	The startup ecosystem of the IoT security market: No. of startups are more than 30% of the existing players. This is bringing new innovations in the market.
R&D	R&D spending of the majority of the players are high in the IoT security market
Mergers and Acquisitions	M&A activities are moderate in the last one year in the IoT security market.

An overview of market dynamics is depicted below, summarizing market drivers, restraints, challenges and opportunities of IoT security industry.

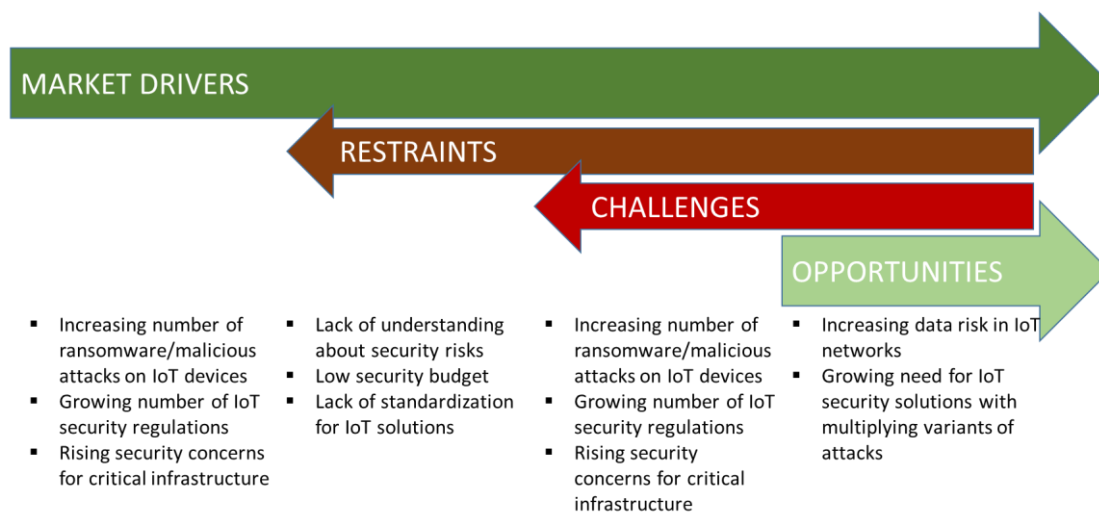


Figure 14: Market Dynamics

Summary of Market Drivers

Malicious attacks **against Internet of Things (IoT) devices and networks** have been escalating throughout the last years with 32.7 million IoT attacks having been detected during last year by SonicWall²³, while phishing saw a decrease in volume with most of the attacks being targeted.

While everyone wants to have their devices interconnected and connected to the Internet, many of the estimated 31 billion IoT devices that will be installed by 2020 according to Statista²⁴ will also come with easy to abuse or no security controls. This allows malicious actors to compromise and add them to large scale botnets they control by exploiting security flaws impacting them in great numbers or taking control of them using publicly available default credentials.

²³ <https://www.sonicwall.com/news/annual-sonicwall-cyber-threat-report-details-rise-in-worldwide-targeted-attacks/>

²⁴ <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>

The fact that IoT manufacturers failed to implement proper security controls to protect this type of devices from remote attacks allowed the number of IoT attacks to increase during last years by 217.5% from the 10.3 million logged by SonicWall²⁵ in 2017 according to its 2019 Cyber Threat Report.

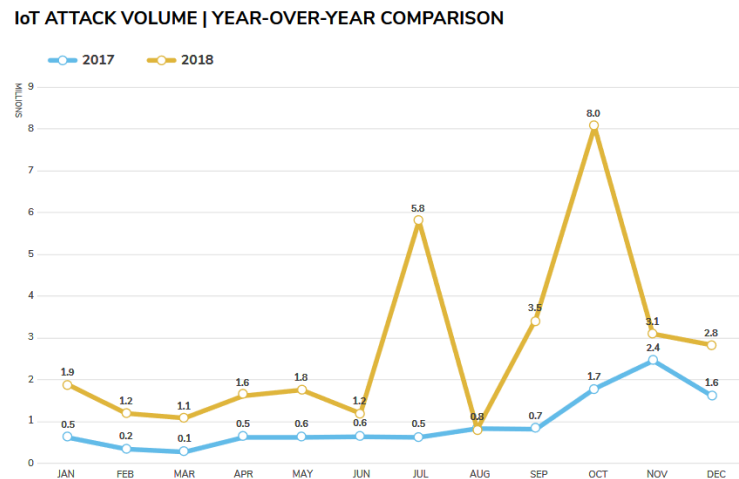


Figure 15: IoT Attack Volume

There is no question that the uptake of network-connected devices that interface with the physical world as sensors and actuators has grown dramatically. As the uptake of IoT has increased, the number and laws of calls for meaningful **IoT regulations** has grown in parallel²⁶.

IoT devices have also enveloped the segment known as **industrial control systems** that has been a mainstay of manufacturing, power generation and delivery, water systems, and a wide variety of other industrial applications for decades. While the industries those devices supported may have been subject to a wide array of safety, environmental and sometimes cybersecurity regulations, the devices themselves were regulated indirectly, if at all. If the purchasers of those devices were in regulated industries, such as electric power delivery, healthcare or financial services, they were obligated to ensure that the devices they purchased, when combined with their own people, processes and technology, provided adequate security.

As the Internet of Things market has exploded beyond the traditional industrial control and medical device market, there has been increased interest in **directly regulating** the devices themselves now that technically unsavvy consumers are in the mix. For example, in USA the Security and Privacy in Your Car (SPY Car) Act is proposed to address security and privacy protection in automobiles. While this and similar legislation have yet to gain much traction, it is likely that the media attention over recent cyberattacks involving IoT devices will eventually force legislative or regulatory action at the state or federal level, particularly if the cyberattack leads to death or serious injury. Consequently, it is important that the industry strives to both influence and respond to the likely changes in the legal landscape.

Another key market drivers is the **rising security concerns regarding critical infrastructures**. What we think of as the critical infrastructure is influenced by the industry a company operates. In the financial industry, for instance, the critical infrastructure might focus on credit card

²⁵ <https://www.sonicwall.com/news/annual-sonicwall-cyber-threat-report-details-rise-in-worldwide-targeted-attacks/>

²⁶ <https://www.iotworldtoday.com/2017/04/11/iot-regulation-disarming-ticking-security-time-bomb/>

systems and online banking operations. In many cases, however, a larger scope of the critical infrastructure is adopted as defined by EU²⁷:

Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behavior, may have a significant negative impact for the security of the EU and the well-being of its citizens.

Given the breadth of this definition, critical infrastructure is at risk of attack against all three categories of cybersecurity risk: confidentiality, integrity and availability. Much of the focus in the media is on protecting the availability of these services: what happens if the grid goes down, or connectivity is lost to critical services. However, attacks on the integrity of these services will become a bigger challenge as actors seek to influence how data-driven decisions are made. As in any other type of network infrastructure, the risks come because the attacker knows where the fault lines are. The critical infrastructure is not any different. The APTs are spread by phishing attacks. Critical infrastructure may also fall victim to rogue or unaware insiders that leave corporate assets exposed.

The challenge in protecting the critical infrastructure from cyber threats is twofold. First, the **complexity** and **diversity of the infrastructure** requires covering and supporting an immense breadth of tools, platforms and applications. There is a delicate balance in keeping systems resilient and updated and running. The second aspect of this challenge is one of focus. So much investment is being made in the availability of these resources that risks to the confidentiality and integrity of the data that supports these services get triaged at a much lower priority. These services need to protect access to core data and establish a clearer way to trust actors manipulating that data.

Summary of Market Restraints

An explosion of IoT adoption during the last years gained the attention of cyber criminals, who now consider this technology as "easy prey" given the majority of exploits center on weak passwords or unpatched software.

The first Internet of Things threat that emerged nearly two decades ago looked a lot like the IoT threats observed for the next 12 or so years. But in the last few years, the development of malware targeting IoT devices has increased as shown in the figure

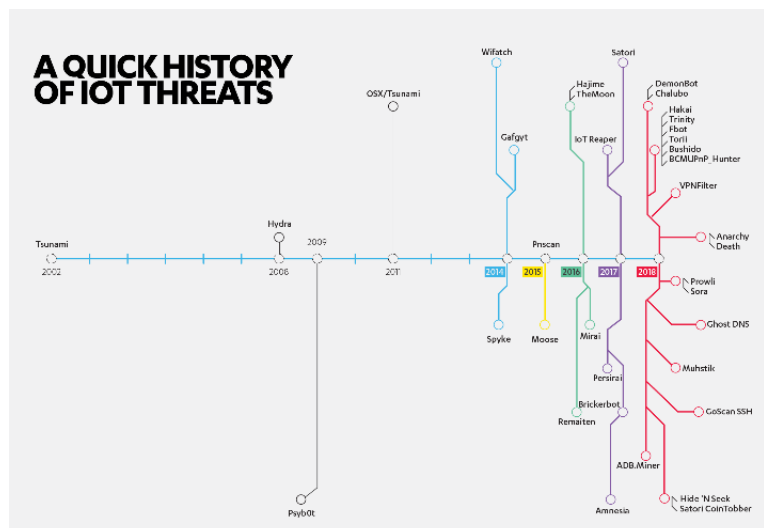


Figure 16: IoT Threats History

²⁷https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

below²⁸, an indicative representation of the growing trend in number and variety of IoT threats. To get a sense of a scale of the problem, a 10-year-old vulnerability discovered in 2018 left as many as half a billion IoT devices vulnerable²⁹.

Lack of awareness, regarding security risks that affect IoT, complicates the decision-making process for investing in the proper IoT cybersecurity solutions. Decision makers either do not know much about the IoT or they do not realize the possibility to be affected and suffer the financial impact of no compliance to regulations.

It should be prioritized to provide all the **fundamental knowledge regarding IoT**, connected devices, and the threats to every individual. Having basic knowledge about the impact of IoT and its security threats could be the difference between having a safe network and a data breach.

Over the years, Internet users have learnt how to avoid spam or phishing emails, perform virus scans on their PCs, and secure their WiFi networks with strong passwords. But IoT is a new technology, and people still do not know much about it. While most of the risks of IoT security issues are still on the manufacturing side, users and businesses processes can create bigger threats. One of the biggest IoT security risks and challenges is the **user's ignorance and lack of awareness of the IoT functionality**. As a result, everybody is put at risk.

Tricking a human is, most of the time, the easiest way to gain access to a network. A type of IoT security risk that is often overlooked is social engineering attacks. Instead of targeting devices, a hacker targets a human, using the IoT.

An effective IoT security solution should prevent attacks on corporate cyber-physical device fleets that are part of the broader IoT world. The key requirements include i) device and data security, including authentication of devices and confidentiality and integrity of data, ii) implementing and running security operations at IoT scale, iii) meeting compliance requirements and requests and iv) meeting performance requirements as per the use case. These requirements make an **overall IoT security solution expensive** in a restricted-budget environment that most of companies operate.

Summary of Market Opportunities

More information creates more possibilities to create value³⁰: This is the promise of the IoT. Today, entire business models are launched on the idea of tight collaboration between organizations – and data is often the glue holding them together, propelling companies to invest significantly in customer analytics capabilities to discover new value streams for their customer.

²⁸ F-Secure, IoT Threat Landscape

²⁹ IoT Security Flaw Leaves 496 Million Devices Vulnerable At Businesses: Report <https://www.crn.com/news/internet-ofthings/300106806/iot-security-flaw-leaves-496-million-devices-vulnerable-at-businesses-report.html>

³⁰ Deloitte, Flashpoint: Cyber risks in an Internet of Things world

These collaborations are taking advantage of an exceptionally broad portfolio of data types—not just device and system data, but everything from employee rosters and inventory records to non-traditional data types such as facial recognition data, facilities access data, industrial control system data, to name just a few. For many, this is uncharted territory, and along the way, data governance has failed to keep pace, highlighting the **importance and necessity of overall security**.

The rapid adoption of new data technologies has made **data risk** a more pervasive concern for organizations in nearly every industry, especially those who utilize IoT networks. While addressing the concerns around privacy and ethical use have become top of mind, businesses will continue on the path of digitization and become more data-driven.

Strong data management and a thorough understanding of related risks are critical to managing trust with IoT data, both from within the organization and externally. By aligning and establishing standards on critical data sources across the enterprise, organizations can identify and protect core data assets and any risks to those assets, while creating new value opportunities.

The Internet of Things has access to organizations existing operational technology (OT) networks and information technology in addition to multiple devices, sensors and other smart objects. **Increasing dependence on the existing network connectivity** gives rise to challenges including security threats. The priority and focus of the IT network is to protect data confidentially and secure access, ensuring operational and employee safety. Thus, there is an increased demand for **IoT security** solutions at workplace as shown by market forecasts.

The IoT security opportunity may help IoT security companies expand into new markets along the value chain. They may especially find opportunities within the middle layers of the technology stack, between application and hardware, such as software infrastructure, gateway communication, and communication protocols. However, this is new ground for most companies and competition will be tough, since many other players, including start-ups and strong incumbents from adjacent markets, are trying to develop security solutions for these layers in response to malicious attacks that take advantage of vulnerabilities in these domains.

Summary of Market Challenges

Cybersecurity is on every manufacturer's mind these days as more machines are connected and more groups and alliances emerge as a way to promote security standards and best practices for automation applications. But this trend is not true for company owner, especially for SMEs, and decision makers regarding the impact of security risks in their business. Budget restrains deteriorate the negative impact furthermore, postponing potential investment in cybersecurity.

Meanwhile, the number of cyberattacks, data breaches and overall business disruption caused by unsecured IoT devices are increasing because companies do not know the depth and breadth of the risk exposures they face.

The main security risks associated with the current IoT environment include³¹:

1. Not having a security and privacy program
2. Lack of ownership/governance to drive security and privacy
3. Security not being incorporated into the design of products and ecosystems
4. Insufficient security awareness and training for engineers and architects
5. Lack of IoT/IIoT and product security and privacy resources
6. Insufficient monitoring of devices and systems to detect security events
7. Lack of post-market/implementation security and privacy risk management
8. Lack of visibility of products or not having a full product inventory
9. Identifying and treating risks of fielded and legacy products
10. Inexperienced/immature incident response processes

IoT is known to be marred with issues of reliability and security³². The whole IoT industry is facing enormous challenges, which are growing in severity as its adoption increases and evolves. Vulnerabilities across IoT devices provide easy access to hackers, leading to further malicious attacks, data theft, destruction of data, damage to the hardware. Furthermore, “pwned” devices facilitates largescale coordinated attacks on IT infrastructure, the impact of which is can be felt across geographic boundaries by victims.

The rapid development of technology currently revolves significantly around Internet of Things (IoT) and expected to play an important role in coming years. IoT has become the focus of attention for many researchers to discover issues and challenges that **related to its design and architecture**. One of the many significant issues is the multitude of languages, protocols and standards, as well as the lack of agreement on which it works best for individual layers of the IoT. It does not have a single platform of standardization; it is changed due to the heterogeneity of connected things. The lack of standardization has high impact on security, interoperability and governance domain, affecting consequently the effectiveness and adoption of IoT security market as a whole.

Standardization describes how the different parts of the technology stack should interact. Instead, large players and industry organizations use their own solutions. Some segments, such as industrials, still rely on a small set of proprietary, incompatible technology standards issued by the major players, as they have done for many years. In other segments, such as automotive or smart buildings, standards are rudimentary. This lack of standards may slow IoT adoption or discourage device manufacturers and others from developing new technological solutions, since they do not know whether their innovations will meet the guidelines that eventually become dominant. In addition, IoT and IoT security players will have difficulty developing end-to-end security solutions without common standards.

³¹ TechRepublic, Securing IoT in your organization: 10 best practices

³² Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, and Dechao Qiu. 2014. Security of the Internet of Things: Perspectives and Challenges.

3.6 Stakeholder Analysis

The stakeholder analysis identifies customers, groups, and institutions that have an interest in the results of C4IIoT. A clear overview of stakeholders and their goals, interest and influence is an important precondition for analyzing the context and market for C4IIoT, for formulating value propositions and identifying optimal communication channels.

We have identified the following stakeholders:

- Automation and control system providers
- Security regulatory authorities
- IoT hardware manufacturers
- Managed service providers
- Cloud service providers
- Telecommunication service providers
- Information Technology (IT) security agencies
- Third-party system integrators
- Consultancy firms/advisory firms
- IoT security professionals and consultants
- Investors and venture capitalists
- Managed service providers and middleware companies
- Data management and predictive analysis companies
- Internet identity management, privacy, and security companies
- Machine-to-Machine (M2M), IoT, and telecommunications companies

Analyzing stakeholders is crucial for any project/initiative to understand relevant actors' needs, desires and potential barriers to a specific implementation, development or change. By assessing the needs of each category, proactive steps can be taken to ensure affected/affecting actors would work synergistically with the goals of the project and do not undermine its success. The capability to identify and deliver benefits consequential to the engagement in for the most relevant stakeholders, exponentially increases the probabilities of success and large-scale deployments.

This stakeholder analysis uses a common Power/Interest approach (Mendelow, 1991), which divides the stakeholders in 2 groups (primary and secondary stakeholder). The main difference between primary and secondary stakeholders is that C4IIoT success directly depends strictly on the involvement and cooperation of the first ones. Primary stakeholder may show more or less interest on project outcomes, but they have higher influence and power than the secondary stakeholders and their aversion could lead to project failure.

High power, high interest stakeholders are key players. Low power and low interest stakeholders are least important. Depending on the classification of different stakeholders, different engagement strategies should be implemented.

Level of importance	Category & classification	Strategy to maximise their engagement
Primary stakeholders	1. Key players: High Influence & High Interest	<ul style="list-style-type: none"> • Key players focus effort on this group • Engage and consult regularly • Involve in governance
	2. Meet their needs: High Influence & Less Interest	<ul style="list-style-type: none"> • Engage and consult in their interest area • Try to increase level of interest • Aim to move into key players
Secondary Stakeholders	3. Show consideration: Less Influence & High Interest	<ul style="list-style-type: none"> • Make use of interest through involvement in low risk areas • Keep informed and consult on interest area • Potential supporter
	4. Least important: Low Influence & Low Interest	<ul style="list-style-type: none"> • Inform via general communications: Newsletter, website, etc. • Aim to move into group 3

Figure 17: Classification of stakeholder types with associated strategies for engagement

The goal of stakeholders' analysis is to highlight what are the needs, challenges, barriers and benefits of each listed stakeholder with respect to the successful diffusion of C4IIoT and provides meaningful information to the consortium, in order to take appropriate actions to approach each stakeholder following the ideal communication strategy.

Table 2: Stakeholders' analysis

Actor	Primary	Secondary	Needs – Challenges and Benefits
Automation and control system providers	<input type="checkbox"/>		<ul style="list-style-type: none"> ▪ International Harmonization and Interoperability ▪ Improvements to framework policies and the development of international standards ▪ Network resilience
Security regulatory authorities	<input type="checkbox"/>		<ul style="list-style-type: none"> ▪ Promote Software Best Practices ▪ Promote Shared Responsibility ▪ Develop Tools to Inform end users
IoT hardware manufacturers	<input type="checkbox"/>		<ul style="list-style-type: none"> ▪ International Harmonization and Interoperability ▪ Lower cost, better margins
Managed service providers		<input type="checkbox"/>	<ul style="list-style-type: none"> ▪ Communication protocols ▪ Data encryption ▪ Automation and management tools
Cloud service providers		<input type="checkbox"/>	<ul style="list-style-type: none"> ▪ Data integrity ▪ Privacy and confidentiality ▪ Strong encryption mechanism
Telecommunication service providers		<input type="checkbox"/>	<ul style="list-style-type: none"> ▪ New communication protocols ▪ Data integrity

Information Technology (IT) security agencies		<input type="checkbox"/>	<ul style="list-style-type: none"> Automation and management tools Risk mitigation
Third-party system integrators		<input type="checkbox"/>	<ul style="list-style-type: none"> Market expansion Security awareness Flexibility and Adaptability
Consultancy firms/advisory firms		<input type="checkbox"/>	<ul style="list-style-type: none"> Raising awareness
IoT security professionals and consultants		<input type="checkbox"/>	<ul style="list-style-type: none"> Internet and cloud- powered data analytics
Investors and venture capitalists	<input type="checkbox"/>		<ul style="list-style-type: none"> Effective security Quick ROI Decreasing cost of sensors and software
Managed service providers and middleware companies		<input type="checkbox"/>	<ul style="list-style-type: none"> Standardization Minimized complexity
Data management and predictive analysis companies		<input type="checkbox"/>	<ul style="list-style-type: none"> Identity and access management Secure analysis environment
Internet identity management, privacy, and security companies		<input type="checkbox"/>	<ul style="list-style-type: none"> Quick response to incidents Predictive analytics
Machine-to-Machine (M2M), IoT, and telecommunications companies	<input type="checkbox"/>		<ul style="list-style-type: none"> Standardization Common communications protocols Security by design Lower consumption Adopt standards for testing and evaluation of IoT products

4 Competitor Analysis

The internet of things is growing at breakneck pace and may end up representing a bigger economic shift in networking than the internet itself did, making security threats associated with the IoT a major concern. This worry is reflected by investments being made by traditional players (namely incumbents) and in startups that focus on stopping threats to the IoT, the industrial IoT (IIoT) and the operational technology (OT) surrounding them.

4.1 Incumbents competitive landscape

Two of the most prominent players in the market are IBM (through IBM Research Lab) and Infineon Technologies that are members of C4IIoT consortium, offering with the range and depth of their offerings and their expertise to the successful implementation of the projects, supplementing the contribution of the rest members.

In particular, **IBM** intends to build a decentralized access management solution using HyperLedger fabric (Blockchain). The goal of the application is to enforce data privacy policies. Specifically, to verify that each data transaction has consent from the data subjects to the purpose for which it is going to be used. By utilizing the previous asset, IBM aims at targeting the domains of decentralized privacy-aware access control and Blockchain technologies. The **IBM Research Lab** in Haifa is working closely with the IBM brands and incorporate innovations into their products.

In parallel, **Infineon Technologies** anticipates to facilitate the design and deployment of secure systems by developing simple-to-use standard hardware secure elements, which can be nearly “plug-and-play” into IIoT elements, enabling high-end security and credential management. The project offers the ideal environment to achieve this goal, with the right partners, use-cases and a relevant testbed environment to test and further develop their secure elements. Their main market is the manufacturers of IIoT devices (gateways, routers, sensor nodes, actuators, computing elements, etc.), which may require the high-level of security and trustworthiness achieved by including Infineon secure elements in the design of their products. Their expected benefits through their participation in the project include:

- Increasing their expertise in realistic IIoT deployments and how customers want to use their products.
- Understanding novel requirements for hardware security chips, identifying and fixing potential weaknesses and missing features.
- Acquiring experimental experience in Blockchain platforms, and their use in IIoT environments in combination with their hardware security elements.

Other key players of the market are:

SYMANTEC CORPORATION: Security is one of the key aspects when it comes to an IoT infrastructure where multiple endpoints, servers, gateways, and other elements of the IoT ecosystem are prone to threats from several malicious attacks. The company offers various products and solutions for data and information theft protection at multiple nodes such as endpoints, security over cloud, email security, IT management and security, embedded security,

data center security, control compliance suite Symantec code signing certificates, and secure app service. To ensure the security of the information flowing across the IoT infrastructure, Symantec offers several information protection solutions such as data loss prevention, encryption, access management, and management of PKI services.

TREND MICRO INCORPORATED: The company offers its solutions in 3 major categories, namely, cloud security, endpoint security, and email and mobile security. In cloud security, the company offers 3 products: Trend Micro Deep security platform, Trend Micro smart protection, and network and cloud app security. In end-point security, the company offers solutions such as vulnerability protection, endpoint application control, data loss prevention, endpoint encryption, server protect for Windows/Netware, and server protects for Linux. In mobile security space, the company offers hosted email security, and interscan is messaging security to its commercial clients.

TRUSTWAVE HOLDINGS INC: The company offers several services for security and prevention of intrusions and data theft in the IoT network. Trustwave Threat Management services help effectively prevent newer and targeted threats designed to steal valuable information related to business, customer database, and payment card data. Company's threat management service gives better operational insight, quicker detection, real-time protection, and better threat mitigation approaches. The threat management services help carry out threat analysis and security analytics and provide actionable insight based on threat intelligence.

VERIZON COMMUNICATIONS INC: The company offers mobility products and services which include mobile workforce management, mobile application management, M2M solutions, cloud solutions comprising cloud and data center, and security services. In the IoT security space, the company provides products such as cloud security, identity and access management, threat and vulnerability, and risk and compliance. Furthermore, the company also offers software-defined perimeter service, a Software-as-a-Service (SaaS) solution which provides authorized, content-monitored, and secure access to enterprise applications and allows users to identify and avoid cyberattacks by making a virtual boundary around the network.

PTC INC: In IoT security, the company operates with its dedicated IoT security product, Axeda. Axeda helps integrate an end-to-end security mechanism, which spans all levels of an IoT framework namely: network, application, end-user, and data security. Axeda has received ISO 27001:2013 certification, which depicts company's focus on providing the optimum level of security and performance. Additionally, Axeda M2M cloud service helps maintain network security at the client location, protects data from unauthorized entities, facilitates with secure infrastructure, ensures user authentication, user access control management, and ensures granular policy management.

DIGICERT: In IoT security space, the company offers various solutions and services to its commercial clients. These solutions include provisioning and deployment, device identity management, data and system integrity, and secure hosted security module solution for private key management. The company's product offerings are categorized as per industries, namely, healthcare, automotive, industrial, smart city, home and consumer, transportation. It also provides high-volume certificate issuance platform, which can be used to manage the lifecycle of the connected devices.

4.2 IoT Startups competitive landscape

As internet-connected hardware proliferates, there's been a corresponding rise in cyber security threats, with malicious hackers using these new digital entry points to infiltrate and disrupt systems. In turn, startups focused on securing the Internet of Things (IoT) and the Industrial Internet of Things (IIoT) are emerging as important players in the cybersecurity industry.

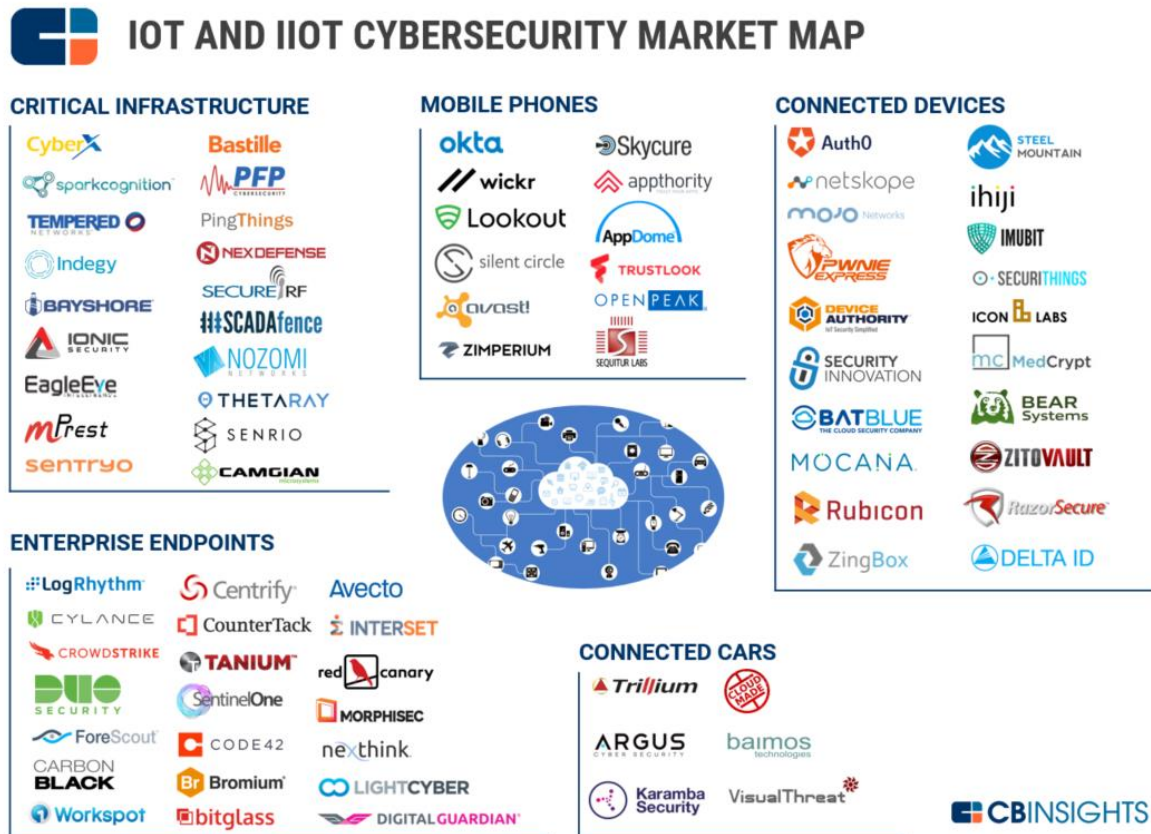


Figure 18: IoT-IIoT Cybersecurity Map

CB Insights³³ has identified 78 private companies at the intersection of cybersecurity and connected hardware, which includes: critical infrastructure, mobile phones, connected devices, enterprise endpoints, and connected cars.

The breakdown of categories is as follows:

Critical Infrastructure: Startups in this category include **Indegy** which provides real-time situational awareness, visibility, and security for industrial control systems used across critical infrastructure, including energy, water utilities, petrochemical plants, manufacturing facilities, etc. Similar companies such as **CyberX** can detect network anomalies by analyzing the operational behavior of industrial internet networks using Big Data and Machine Learning. The company **Bastille Networks** is among the more unique startups in this category, with a product

³³ <https://www.cbinsights.com/research/cybersecurity-iiot-market-map/>

that scans air space to provide visibility into RF-emitting devices. Bastille has broad implications across the connected hardware cybersecurity market.

Mobile Phones: Companies in this category include three unicorns valued at \$1B+. They are: **Okta** which offers cloud-based identity management and mobility management services, **Lookout** which is a smartphone security company for the Android and iOS platforms, and **Avast Software** which offers security and privacy solutions also for iOS and Android.

Connected Devices: Included are companies like **Mocana** which secures IP addressable devices as well as the information, applications, and services that run on them. Companies in this category also include **MedCrypt** which offers the ability to manage all of the digital keys needed for users to securely access medical devices.

Enterprise Endpoints: Startups like the unicorn **Tanium** offer a systems management solution that allows enterprises to collect data and update endpoints across networks. Another unicorn in this category is **Cylance**, which operates in defense of enterprises' endpoints by applying artificial intelligence algorithms to predict, identify, and stop malware and advanced threats.

Connected Cars: **Argus Cyber Security** enables car manufacturers to protect technologically advanced connected vehicles from malicious cyber-attacks.

4.3 Industrial IoT Startups landscape

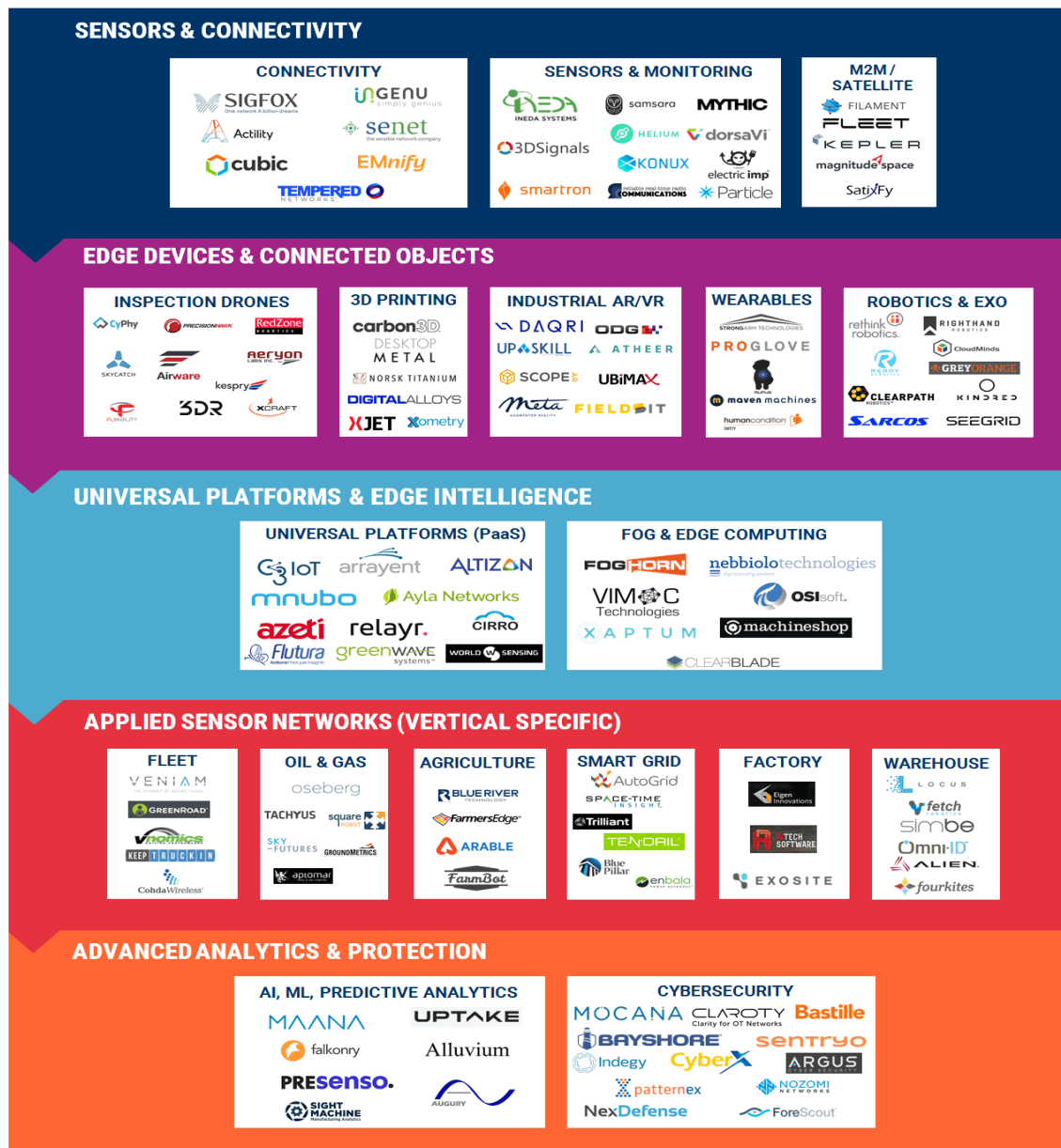
So far, the IIoT wave has been led by the old guard of industrial tech companies such as GE, IBM, and Cisco, who envision the IIoT as a core component of their future businesses. GE, in particular, pioneered the term “Industrial Internet” when announcing its \$1.5B R&D commitment back in 2012³⁴.

But more and more startups are attacking the needs of heavy industry by developing sensors, cloud platforms, networking infrastructure, as well as machine learning software to extract insights from the deluge of data. An overview of the startup landscape within IIoT is depicted in the following figure, with a new approach that categorizes companies by where they sit in the tech “stack,” starting from hardware all the way down to AI-powered analytics³⁵.

³⁴ <https://www.technologyreview.com/s/507831/general-electric-pitches-an-industrial-internet/>

³⁵ CB Insights - <https://www.cbinsights.com>

THE INDUSTRIAL IOT (IIOT) STACK: 125+ STARTUPS BRINGING DIGITIZATION TO HEAVY INDUSTRY



CBINSIGHTS

Figure 19: IIot Start-ups

The category breakdown introduced by CB Insights is as follows:

Sensors & Connectivity

- **Connectivity** — wireless network providers like **SigFox** and **Ingenu** act as the telecoms for the IoT age. Most companies here provide LPWAN (low-power wide area network) connectivity, which is popular radio band for IoT devices because existing cellular systems aren't power- and bandwidth-efficient enough for systems sending small packets of data. Some, like **Senet** use the LoRaWAN spectrum, and others like **SigFox** work with ultra-narrowband specifically for low-power devices.

- **Sensors & Monitoring** — some companies in this area are solely sensor or system on chip (SoC) makers like **Ineda Systems**, but the category also includes more “full stack” (but industry agnostic) sensor and monitoring platforms like **Samsara**, **Helium**, and Electric Imp.
- **M2M / Satellite** — sometimes Industrial IoT assets operate in rural and less connected parts of the world. Satellites can be a more effective way for sensors to transmit data, and companies like **Kepler Communications** offer a space-based communication network. With similar advantages in isolated industrial environments, machine-to-machine (M2M) communication is a more decentralized way to pass information between devices, and companies like **Filament** are applying blockchain architecture to do so with low-power industrial sensors.

Edge Devices & Connected Objects

- **Inspection Drones** — startups offering drone hardware or image analysis services for industrial inspection. Some startups like **Skycatch** have individual use cases, such as construction. Recently, drone makers famous for their consumer drones like **3D Robotics** have moved into the inspection space. While it’s mostly aerial drones for now, the category encompasses all types including underwater drones and pipe inspecting drones such as those made by **RedZone Robotics**.
- **3D Printing** — leveraging materials science and robotics, companies like **Desktop Metal** and **Carbon 3D** are bringing the customization benefits of 3D printing to an industrial scale. 3D printing tech is starting to go beyond just prototyping tools to being production-scale for making parts, which is why corporate venture arms of GE and BMW are investing here.
- **Industrial AR/VR** — headsets and mobile AR specifically tailored for industrial settings and field service. **Daqri** and **Atheer** are well-funded headset makers that focus on enterprise and industrial settings. Others like **Scope AR** do similar work in field service using mobile and tablets, employing AR to highlight parts on industrial equipment while connected to support experts in real-time.
- **Wearables** — IoT sensors worn on the body in industrial environments. **Strong Arm Technologies** makes a safety wearable and some industrial smartglass makers like **Ubimax** and **Upskill** also have wearables offerings.
- **Robotics & Exo** — industrial automation robots along with exoskeletons that augment human abilities. Companies like **Rethink** and **Righthand Robotics** both make the classic arm-shaped industrial robots for manufacturing. **Clearpath Robotics** does warehouse robotics, as well as a host of ruggedized ground and sea-faring drones. And companies like **Kindred** and **Sarcos** are developing worker exoskeletons that can help handle heavy materials or be remotely operated for inspections.

Universal Platforms & Edge Intelligence

- **Universal Platforms** — cloud vendors here commonly market themselves as general platform-as-a-service (PaaS) companies that allow other IoT and IIoT companies to manage and maintain the capture of data from their device networks. This includes the mostly industry-agnostic platforms like **C3 IoT** and **Altizon** that do cloud analytics for industrial companies.

- **Fog & Edge Computing** — computing done at the “edge” or closer to the sensor is a trending shift occurring within the IIoT architecture. Companies like **Saguna Networks** do edge computing (close to the point of collection), whereas a company like **Foghorn Systems** does fog computing (think a lower-hanging cloud that’s done on-site like a LAN). Both methods allow mission-critical devices to operate safely without latency of transmitting all data to a cloud, which can also save big on bandwidth.

Applied Sensor Networks

- **Fleet** — sensor networks and solutions for connected trucking fleets. Companies like **Veniam** are focused on the connectivity aspect, where others like **Vnomics** sell optimization and vehicle monitoring technology.
- **Oil & Gas** — companies using connected sensor networks in the oil industry include **GroundMetrics** (locating wells), **Tachyus** (extracting oil and gas), and **Aptomar** (spill safety).
- **Agriculture** — companies like **Blue River Technology** and **Farmbot** are bringing robotics to agriculture. Others like **Farmers Edge** and **Terravion** are about capturing and analyzing farm data and tractor telematics for more efficient production.
- **Smart Grid** – startups in this area develop tech that enables more efficient distribution of electricity, gas and water, and often market to utility companies. **Trilliant**, **Tendril**, and **BluePillar** are smart-meter enabled solutions for utilities and large enterprises to manage usage and reporting.
- **Factory** — **Eigen Innovations** and the companies in this category are more vertical-specific platforms for manufacturing analytics. Eigen, for example, uses video and sensor data on factory floors to ensure process and quality control.
- **Warehouse** — robotic movers and RFID sensor systems that target the warehouse. **Fetch Robotics**, for example, does material transport on warehouse floors. **Alien Technologies**, one of the most well-funded startups in all of IoT, does RFID tagging tech for the supply chain.

Advanced Analytics, Edge Intelligence & Protection

- **AI, ML, Predictive Analytics** — software that allows companies to find insights and derive predictive analytics such as when machines will need maintenance. Most companies in the category are like **Maana** and work by applying AI to mining machine data, but others, like **Augury Systems**, offer a full sensor suite that detects machine anomalies and offers predictive analytics.
- **Cybersecurity** — companies in this category develop cybersecurity solutions for IIoT and industrial control systems (ICS) in heavy industry. The IIoT has already suffered serious hacks; a German steel mill suffered “massive damages”³⁶ after hackers accessed a blast furnace that workers could not properly shut down. **Bastille Networks** is one company that focuses on protecting the wireless transmission of IoT and RFID devices, and **Claroty** is a well-funded company working on protecting industrial control systems.

³⁶ <https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>

5 Identifying C4IIoT Competitive Advantage

5.1 PEST Analysis

The PEST (Political, Economic, Social, Technological) analysis is a strategic business tool to discover, evaluate, organize, and track macro-economic factors which can impact on C4IIoT outcomes now and in the future. The framework examines opportunities and threats due to Political, Economic, Social, and Technological forces and helps the consortium to get a comprehensive picture of the status and trends of important factors that are beyond its control but have an impact on the project.

Although the outcomes of C4IIoT, and the security framework that it proposes, will increase the overall security of IIoT schemes, it will contain some sticking points that governments, labor and society may contest. The overall analysis of previous chapters regarding the market trends, drivers and constraints, help us to better understand the macroeconomic environment and the potentials of C4IIoT.

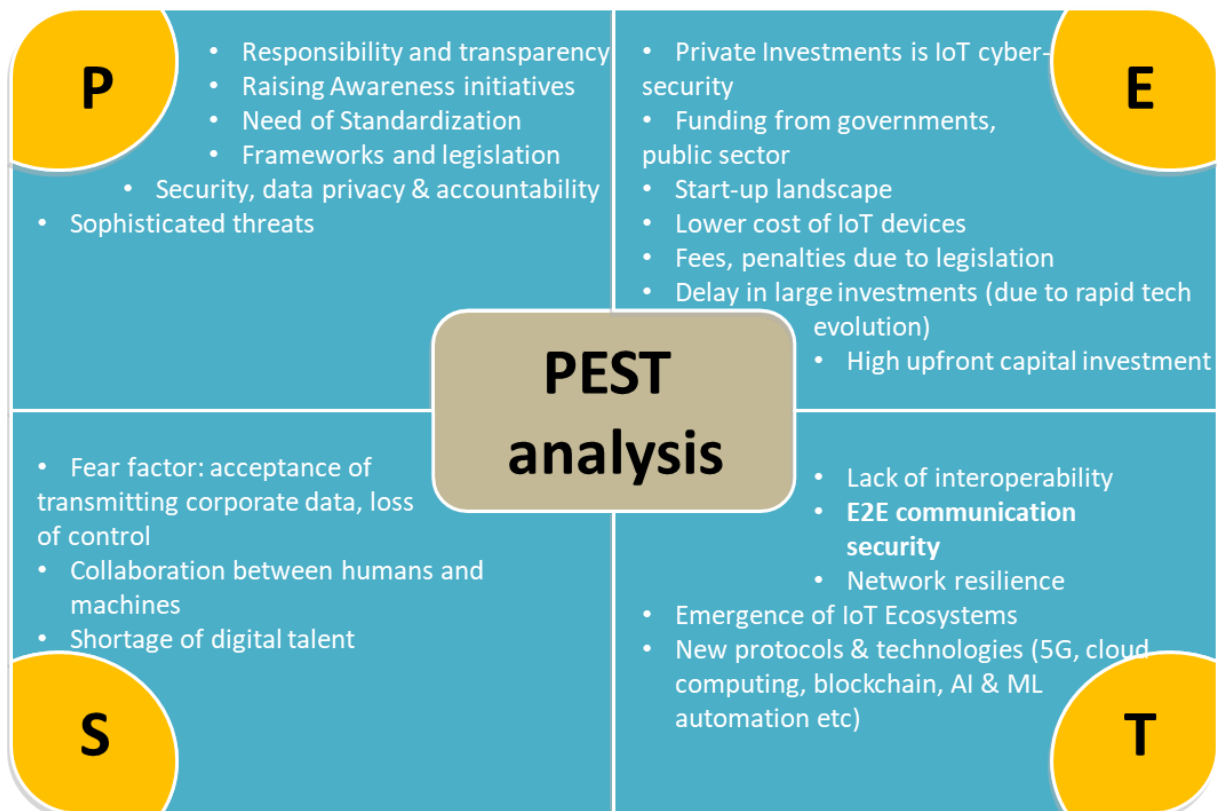


Figure 20: PEST Analysis

Summary of political factors:

Political factors include political stability, government policies, and activities of regulatory bodies and lobbying groups that may affect business through legislation, policies, rules, regulations and directives. Political factors are closely tied to legal factors but are more focused on the underlying drivers and the political process eventually leading to binding legislation.

The main political concerns relating IoT and IIoT cyber-security market has to do with **responsibility and transparency issues**, a dimension that is highly connected with the lack of dominant framework and **standardization** schemes. For many businesses, customer experience is the key. In this context, they are willing to disguise cybersecurity and software procedures in order to deliver a ‘seamless customer experience’. Challenges arise when governments force through legislation and directives companies to be more transparent for their customers and internal processes. Whilst companies may be reluctant to police their users’ data, many are still willing to comply with regulatory and enforcement bodies to maintain safe online environments.

As the IoT blurs the lines between data protection, security, safety and liability, current regulations may need to be adapted and aligned to match this change. Legislation has been designed without an integrated approach to these issues. The implementation of current and forthcoming **regulatory frameworks** will require more coordination and information sharing between the public agencies that monitor the adoption and enforcement of security by default measures.

With IoT devices being attractive in industrial landscape, companies need to know the risks they are taking by bringing them into their production environment. It is the responsibility of both public institutions and private companies to **educate** and **aware** end users and companies in the security controls they should adopt. Service providers have a responsibility to protect user data but must also avoid becoming too intrusive when serving their customers. Public bodies and the private sector have a responsibility to ensure that only IoT devices that adhere to ‘secure by default’ principles enter the market. In order to achieve this, governments might consider making ‘secure by default’ principles mandatory or adopt their own procurement policies that drive this.

A number of aspects of **accountability** should be considered as well: i) is it the device or the human that programmed it responsible when an automated device fails and threatens someone’s safety? and ii) as machine learning becomes more common in autonomous devices, it must be applied appropriately and safely. Autonomous vehicles, for example, that operate without human intervention will demand high levels of accountability, as the consequences of failure could be the loss of human life. IIoT security solutions act as a risk mitigation factor regarding intellectual property, transferable knowledge and data ownership. These new concepts challenge current government structures to legislate for the future of the IoT and automation. Individuals, companies and society first need to understand what is meant by being a ‘digital ontology’ in a networked civilization if government and industry is to take responsibility on their behalf.

In addition, the modern business environment contains increasingly **complex cyber threats** that the authorities struggle to identify in time or tackle. With low awareness level in cybercrime, it is unclear who will respond to it as it becomes more frequent and sophisticated. The cybercrime is everybody’s responsibility not just that of the governments, and industry should use their superior infrastructure and resources to supplement that of the security authorities.

Summary of economic factors

Economic factors include long-term trends of global economy as well as fast market fluctuations, costs and competition, as well as economic implications of political decisions, taxation and legislation. As already highlighted in the previous chapters, **private investment**

in the IoT has mostly been in the development of software for smart homes and buildings and venture capitalists predict the highest return on their investment in the short term. The same trend is valid for industrial set-up too. This focus on software has detracted attention from investment in hardware (a tougher and more expensive challenge), leading to a market containing higher volumes of cheap and insecure hardware that pose security risks.

The IoT security market will likely be shaped by the following factors:

- the desire for cost-effective solutions to expensive services, e.g. healthcare provision in remote areas
- the increasing funding from governments and public sector for the development and exploitation of IoT security initiatives
- the lower cost of IoT devices, their usage and maintenance, improving the ROI of investing in cyber security
- the delay in large investments due to rapid evolution in technology
- the volume of uptake across different markets, e.g. low-cost disposable devices may attract more attention than specialized devices requiring long term investment.
- The economic impact of no compliance with legislation, directives and regulation frameworks.

Summary of social factors

Social factors refer to the economic and social conditions of individuals or groups of the society. These are reflected in attitudes, preferences and trends that can influence market behavior and political decisions and eventually legislation. It is therefore important to understand how social factors may influence market demand, funding possibilities and legislation in order to determine how they may affect future business environment. The relevant social factors and the society of interest will depend from case to case. It is also good to note that the social factors may change quickly, for example, as employment or economic conditions change.

A major concern is the availability of skilled workforce. Europe will face a shortfall of 900.000 IT workers by 2020 and the picture is even worst regarding IT security personnel. Currently the European Commission estimates that 32 percent of Europe's workforce has insufficient digital skills. Other factors include:

- the lack of Transparency regarding who has access to data, corporate or personal
- the willingness to share data with value in case of gaining a clear advantage by sharing them
- the co-existence of human factor and machines in production environments
- skepticism about data protection and the effectiveness of security solutions
- the unequal availability and access to security solutions between larger organizations and SMEs due to budget restrictions
- the dispersed information about security implications mainly between individual owners and smaller companies

Summary of technological factors

Technologies keep developing at accelerating pace. Digitalization of almost all sectors of society and industries has been the dominant trend for quite some time and will continue to challenge conventional solutions by offering increased capacity and lower costs. Digitalization is also the main driver behind the growth of Internet of Things (IoT) that promises to change fundamentally the industrial landscape by providing ubiquitous connectivity and accessibility of information.

Despite IoT promises, a big obstacle still stands – **interoperability** – the key to the viability and long-term growth of the entire ecosystem, especially industrial IoT. It is the biggest hurdle facing the industry and hindering its acceleration. Currently, devices from different brands or even from one single brand, models and generations are incompatible at data and service layer. A substantial development of solutions for a wide range of devices and IoT platforms over the past years has taken place. However, each solution provides its own IoT infrastructure, devices, APIs, and data formats leading to interoperability issues. Such interoperability issues are the consequence of many critical issues such as vendor lock-in, impossibility to develop IoT application exposing cross-platform, and/or cross-domain, difficulty in plugging non-interoperable IoT devices into different IoT platforms, and ultimately prevents the emergence of IoT technology at a large-scale.

In parallel, new and more **complex threats** are arising taking advantage the vulnerabilities of existing IoT sensors. For such to happen and for IoT to assume its position as a potent force, it needs support from various technological developments. What these technologies need to do primarily is not to necessarily support the IoT, but instead as they advance, they are subsequently going to massively boost IoT innovation as a whole.

Among the **evolving and emerging technologies** that are driving the development of IoT are cloud computing, IPv6, 5G, block chain and machine learning to name some. IoT security solutions should be expandable and upgradable to incorporate and take advantage of the adoption of new technologies in production and manufacturing lines.

Reducing security vulnerabilities will remain a primary focus. With the rising number of IoT devices, hackers and cybercriminals are continuously finding new ways to compromise IoT devices and networks. **Multi-layered, end-to-end security** throughout the IoT data chain – from end nodes to the gateway to the Internet and finally end users' application platforms – will be imperative. Advanced Encryption Standard (AES) can be paired with Transport Layer Security (TLS) protocol to enable such a versatile end-to-end security. AES is an open encryption standard widely employed for data link layer encryption in low-power IoT networks, while TLS is an application-layer cryptographic protocol for secure web communications. Adoption of these industry-standard, well-proven solutions is crucial to protect the integrity and confidentiality of IoT data against imminent cyber-threats.

In any environment, IoT systems need to cooperate and coexist. This would lead towards them operating efficiently and productively. Data needs to be shared between various devices and platforms and as a result, a proper **IoT ecosystem** is formed. These ecosystems are developing

rapidly all around the world and major organizations are realizing that. Products and services need to be developed in such a way that they do not hinder the processes in any ecosystem and can be introduced to continuous updates.

Network security and resilience by itself is another critical technological factor that affect IoT cybersecurity landscape. Network breaches can have disastrous consequences, including:

- loss of confidential corporate and customer information
- disruption of network services
- impairment of critical industrial systems, especially physical outputs.

As more IoT devices are brought into workplaces and infrastructure, so are more gateways to private networks. If introduced without consideration of their safety, these gateways provide potential attackers with opportunities to infiltrate these networks. Security measures are most effective at the network level, but only if a full network map exists. This is because organizations that do not know what is on their network will be unable to isolate threats when they appear. IoT devices add complication to network security but the threats are still manageable. If a network owner has knowledge of what is in their network, they can be alerted when an attack is imminent by using devices on the periphery of the network as ‘flags’. This allows time to isolate important parts of the network before extensive damage is done. To be successful, all devices in the network must be properly patched, with network owners understanding that software patches do not necessarily compromise safety simply because of their external origin. Knowing the provenance of firmware upgrades and patches is vital to good cybersecurity. As the IoT expands beyond industry, good industry practices such as detailed network surveillance could be passed onto the growing consumer market.

5.2 SWOT Analysis

This section provides a SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis, listing the internal strengths and weaknesses of the C4IIoT solutions as well as the opportunities and threats faced by C4IIoT due to changes in the external environment. SWOT Analysis is a strategic planning tool for evaluating the above factors for a project or a business venture. This process allows C4IIoT to identify internal and external factors that are favorable and unfavorable to achieve its objectives. More specifically it provides the opportunity to:

- Evaluate the strengths of its situation
- Define the weaknesses, which the consortium will try to minimize later on
- Recognize the possible threats and treat them in a planned and organized way

The following SWOT analysis diagram was derived from the results of the previous sections, supplemented by our vision of project's outcome and the clear understanding of market potentials recognizing the strength and weaknesses of the consortium as a whole as well as the opportunities and the threats of C4IIoT initiative.

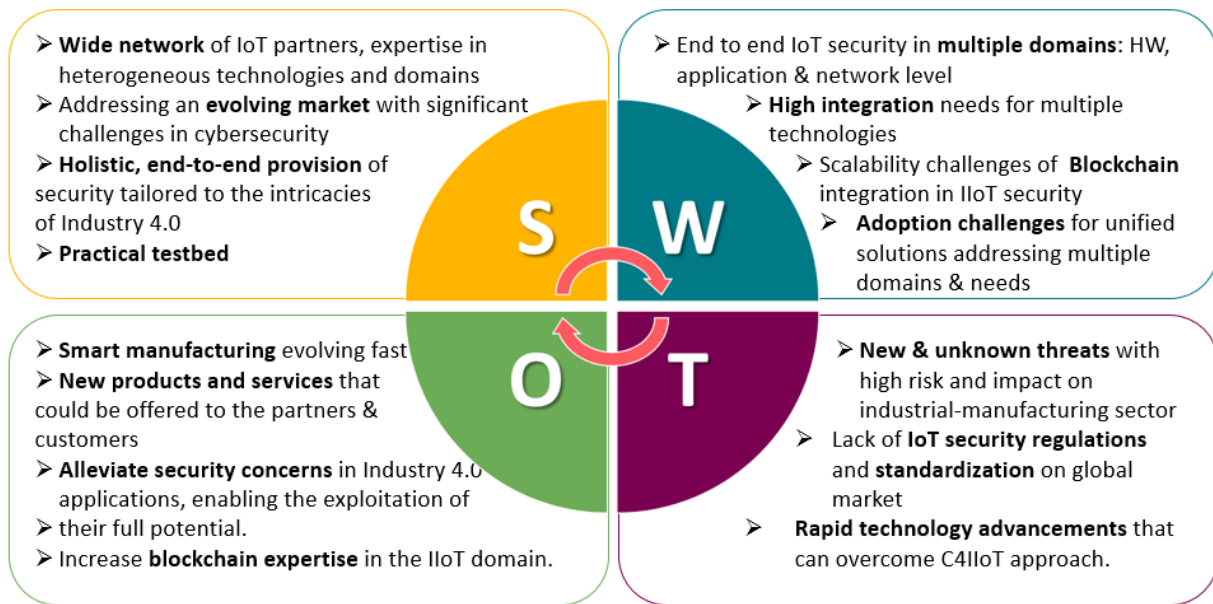


Figure 21: SWOT Analysis

In the annex, there is a detailed SWOT analysis derived by the expertise and market awareness of industrial partners from the C4IIoT consortium. With the common vision of project's outcome and a clear understanding of market potentials every industrial partner recognizes the strength and weaknesses of the consortium as a whole as well as the opportunities and the threats of this initiative.

5.3 Unique Selling Proposition

Based on the conclusions derived through the PEST and SWOT analysis, we can now identify C4IIoT true competitive edge and a Unique Selling Proposition, which will highlight the specific benefits offered by the incorporation of well-established companies in their domains, for the creation and exploitation of an integrated security solution.

C4IIoT will build and demonstrate a novel and unified IIoT cybersecurity framework for malicious and anomalous behavior anticipation, detection, mitigation, and end-user informing. The framework provides **a holistic and disruptive** security-enabling solution for minimizing attack surfaces in IIoT systems, by exploiting:

- emerging security software and hardware protection mechanisms
- state of the art machine and deep learning and privacy-aware analytics
- novel encrypted network flow analysis
- secure-by-design IIoT device fabrication
- blockchain technologies

The vision of C4IIoT is to provide a viable scheme for enabling security and accountability, preserving privacy, enabling reliability and assuring trustworthiness within IIoT applications.

6 Business model

This chapter is about investigate the potential systematic ways for C4IIoT to unlock long-term value for the project outcome while delivering valuable products and services. A business model includes the kind of incentives it is able to create for its users, the distribution networks it is able to tap into and the key partnerships C4IIoT can leverage on. In short, a business model is a holistic framework to understand, define and design the positioning of C4IIoT in the marketplace.

Business model tools can be used in the phases of the business model generation in order to i) map the business model hypotheses ii) test these hypotheses with customers feedback and iii) iterative this process in order to fine-tune and improve the business potentials and dynamics. The result will be an incremental development of a product/service that will reach a minimally viable version. The better the product based on customers' feedback and real-life pilots, the larger the audience it will reach.

6.1 Business Model Canvas

The author of the Business Model Canvas defines the business model in the following way: "It describes the rationale of how an organization creates, delivers and captures value". The main objective of this idea is the joint of the business model development by all members of the organization in a simple and understandable way. The business model is a kind of a strategic scheme, to be introduced in the framework of structures, processes and systems in the enterprise. According to the concept of Business Model Canvas business model consists of nine fundamental elements that show the logic of developing profit for the company. These elements are: Customer Segments, Value Proposition, Channels, Customer Relationships, Revenue Streams, Key Resources, Key Activities, Key Partners, Cost Structure. In order to facilitate the use of this method the special tool was developed. It shows all nine parts of the business model in an orderly fashion.

The business model of C4IIOT is considered to be a multi-sided one, meaning that there is more than one type of customers that have interest on the service provided. During the analysis of the business model canvas, we need to address each building block considering all the different types of customers that the developed platform needs to serve.

Business Model Canvas -

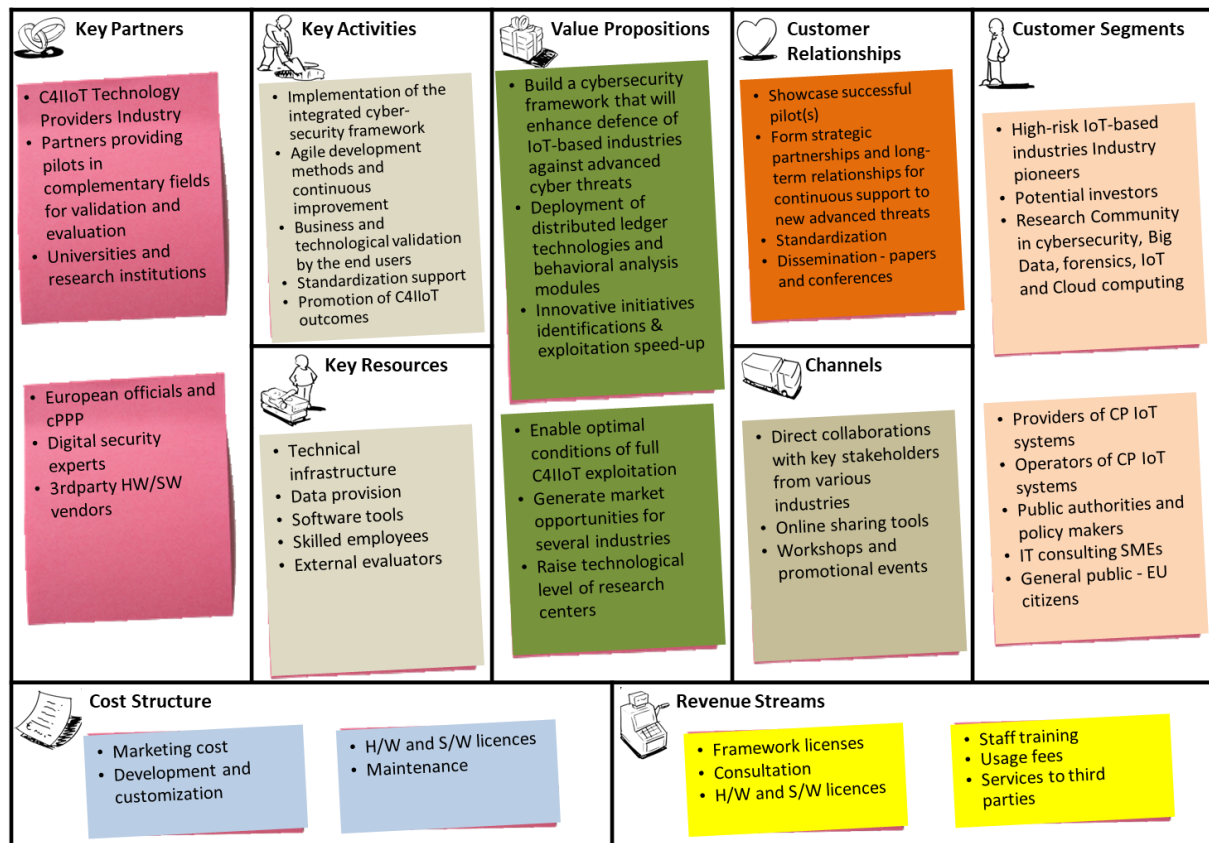


Figure 22: Business Model Canvas

Customer Segments: C4IIoT aims to reach and serve as customer segments high-risk IoT-based industries and industry pioneers, research European community including individual researchers, research centers and universities, providers and operators of cyber physical and IoT-based systems and potential investors interested in new technologies exploitation. The consortium will also actively liaise with public authorities and policy makers to promote the value of the C4IIoT platform.

- **For whom are we creating value?** – We are creating value for the industry and the research community in various sectors. With the implementation of C4IIoT, all potential users in need for better infrastructure or for more mature innovative ideas will be able to contribute in ideas evolution and exploitation via the platform, while at the same time, industry and researchers will interact and share infrastructure, data and needs. Security designers and IIoT planners need to develop solutions with robust embedded cybersecurity and mitigation strategies in case of attack or loss of data. We aspire to set the foundations and disseminate the “security by design” culture
- **Who are our most important customers?** – Important customers will be the industry, especially from the critical infrastructure domains such as manufacturing, energy, digital infrastructure, etc, as well as the research community. Their acceptance, willingness and cooperation in using the platform will be fundamental. This collaboration will lead to the platform evolution and potential investors’ attraction.

- **Where do they live?** C4IIOT will provide a framework able to be adjusted in various industry sectors (manufacturing, logistics, energy, health) and every research community worldwide.

Value Proposition: C4IIOT will be focused on efficiency with high quality and innovative outcome:

- **What value do we deliver to customers?** C4IIOT aims to build a cybersecurity IoT-based framework through which numerous industries from a variety of fields will be able to exploit and enhance their defence in advanced cyber threats. It will provide all interested stakeholders a comprehensive framework of tools, technologies, platforms and services through which they can manage the entire IoT ecosystem with trust and security. C4IIOT also helps market opportunity generation for industry partners, while the research community exploits an upgraded level of technological useful sources.
- **Which one of our customer's problems are we solving?** Fiat Chrysler Automobiles (FCA) is currently managing global platforms with an increasing number of assembly lines, global mix and global demand. Tracking and best utilization are the main issues about containers, combined with the urging need of information accuracy, which cannot be guaranteed if the information is manually inserted in the system without security precautions. Advanced systems for automatic identification and tracking are used, with autonomous, scalable and secure characteristics based on higher ranges and lower power consumption, cellular-like solutions. However, several shortcomings for these solutions have been identified, mainly about the generation of big data and the security. As the devices will be operated both inside and outside the plant, their capacity to be resilient to threats such as intrusion, data modification, device control will be key for the rollout. Industry as well as Research Community, regardless domain, are facing numerous and continuously updated advanced cyber threats. Several stakeholders remain vulnerable to such threats compromising not only their businesses but also the lives of their employees. C4IIOT focuses on providing a platform which will combine the needs of the stakeholders aiming to enhance their defence to such attacks and provide more complete and secure frameworks of operation. We will showcase our approach and technologies in the automotive domain, but we expect upon completion of the project to attract further investments in order to perform wider testing of the platform in different industrial domains that are heavily dependent on IoT.

Channels: Channels describe how a company communicates with and reaches its customers segments to deliver its value propositions. A company can deliver its value proposition to its targeted customers through different channels. Effective channels will distribute a company's value proposition in ways that are fast, efficient and cost effective. An organization can reach its clients either through its own channels (store front), partner channels (major distributors), or a combination of both. For defining the channels, we would need to answer the following questions:

- **Through which channels do our customers want to be reached?** Direct collaboration with industry representatives and research community is one of the main channels. Building an integrated platform and online sharing tools that are easy-to-use will bring C4IIOT framework closer to independent stakeholders. The consortium will also organize workshops and seminar which will also contribute to the promotion of the project outcomes.

- **Which channels work best?** Online channels prove to be a good generator of interest and keeps the relationship with the individual stakeholders.
- **Which ones are the most cost-efficient?** Online channels are the most cost-effective approach.

Customer Relationship Management: C4IIoT aims to build its customer relationships based on strategic partnerships to reach the broader dissemination and exploitation channels possible. It will ensure long-term relationships, providing continuous support to new advanced threats in the IIoT domain.

Revenue Streams: Sources of revenue will be created directly through selling the cybersecurity framework's licenses and through usage fees that will be both subscription and on-demand fees. To promote the framework and engage users, the C4IIoT framework will be offered as a Freemium service, in which a basic version of the framework will be offered free-of-charge, while customized services, enhanced data and advanced visualization on-demand as well as business consulting for the development of a customized framework will be offered for a subscription fee. Revenue streams will also be generated indirectly, i.e. by organizing consultation and training sessions for the users of the framework. During the business planning stage, the project will conduct a cost vs. benefit analysis to determine whether the proposed revenue model needs to be reconsidered. Financial figures and best estimates like the Return on Investment (ROI), net-present value (NPV), sales figures and alike will be provided during the project within the exploitation and innovation plan after a market analysis.

Key Resources: They key resources are: strong partnership research community and industry that will develop and run the framework across Europe. The most important assets required to run the business are software services, an existing technical infrastructure, and skilled human resources providing consulting services. The human capital is identified as the most significant resource for the success of this business plan so every partner plays an important and integral role in the project. Finally, existing software tools (assurance platform; visualization tools; code analysis platform) provided by the C4IIoT partners are also key resources for the project's success.

Key Activities: The key activities will be handled by the C4IIoT consortium are implementation of the cybersecurity framework, development-improvement and support of the framework operation, as well as maintain close relationships with the stakeholders and focus on promoting the framework. Our partners are skilled in these processes and have a lot of experience in running and developing such infrastructures.

Key partnerships: The key partners are the C4IIoT project will design and develop the new described service. Projects Partners satisfy all the categories needed from research and industry community in various sectors.

Cost Structure: C4IIoT incurred costs to operate the business model are costs for the deployment in infrastructure management, software development and maintenance, and marketing. Note that exact data is not provided as they would be purely based on rough

estimates, because essential figures like total cost of ownership (TCO), are still unknown at this point of the project.

To ensure the success of the proposed Business Plan, the consortium has identified a robust set of metrics that will allow us to monitor of success, fine-tune offerings and driving sales quarterly:

Financial reports: Reports will be used to measure the profits and losses along with identifying whether the correct balance of revenue streams is being achieved to meet overheads and grow the business.

Self-awareness check: The consortium will regularly meet to discuss their ideas for the business. As a geographically-dispersed consortium, C4IIoT understands that such face-to-face meetings are critical for ensuring the framework's future matches the vision of the team.

6.2 Barriers to Adoption / Barriers to entry

Barriers to entry are referring to the barriers to digital innovation from start to implementation, as well as assessing the impact of facilitators of ICT innovation. Among the factors that act as a barrier are the following:

- The complexity of regulation landscape.
- Too many divergent interests among the stakeholders entail that digital innovation challenges the ability to cooperate.
- Lack of collaboration by other actors.
- Entry costs to change infrastructures.

There are conditions that improve the degree of success and the terminal alignment with the right ICT infrastructure is key to that. More analytically, barriers to entry the market and hindering the achievement of these impacts do exist, and include the following:

Technological barriers: Information technologies develop rapidly, and it is difficult to foresee their evolution, which may influence technical design decisions. Acting proactively so as to stay ahead of the state of the art and deliver a solution that will not sooner than later become obsolete, C4IIoT will be engaged in a continual technology watch effort by monitoring current research in similar projects and safeguard that the development process will comply with all related standards, will be designed to be flexible and that new requirements that may arise will be properly and timely gathered and processed.

Regulatory barriers: Varying EU states regulations and legal frameworks, with special focus on data protection legislations, may cause setbacks in a pan-European adoption of the C4IIoT approach.

Regulatory Restrictions

Some governments and regulatory bodies are applying existing regulation to IoT products and services in an attempt to influence product security and drive user awareness³⁷.

It is also apparent that particular types of existing regulation and their compliance mechanisms are more applicable than others to security-related risks. This is particularly true for regulations such as consumer protection, competition, product marking or labelling, data protection, cybersecurity, and (tele) communications. The regulatory landscape around IoT is expected to change significantly in the near future, with unpredictable impacts on innovation and the security of legacy devices. National or regional level IoT-specific regulation has yet to be enacted. However, governments and regulatory bodies – such as in the EU, US, UK, and Australia – are known to be developing or considering new legislation specific to the IoT³⁸.

Common sanctions for non-compliance with these regulations could have serious financial and reputational implications for corporations and staff, including fines, personal liability and imprisonment of managers or officers, cease and desist orders, erasure of data, public announcements and product recalls, binding instructions on security features.

The following table summarizes the maximum fines per regulation.

Table 3: Max Fines per Regulation

Regulation	Maximum Fine
General Data Protection Regulation (EU)	€10 million up to 2% global turnover or, €20 million up to 4% global turnover
Federal Trade Commission Act (USA)	\$41,484 (per violation, per day)
Digital Economy Act (UK)	£20,000 a day not to exceed 10% of gross revenue
Privacy Act 1988 and Notifiable Data Breaches Acts (Australia)	A\$420,000 (individuals) A\$2.1 million (corporations)
Health Products Act (Singapore)	S\$50,000 (individuals) S\$100,000 (corporations)

A very recent example of EU's GDPR fine has reached a landmark moment: the first large-scale penalty has been announced, with British Airways facing a fine of £183 million (on the day the fine was announced, equivalent to just short of \$228 million) for a data breach disclosed by the company in Sept 2018. The breach occurred when users of BA's website were re-directed to a fake site, which compromised the personal data of around 500.000 of them. It's the biggest GDPR-related fine so far – by far, and the UK's data protection body – the Information

³⁷ Federal Trade Commission. "ASUS Settles FTC Charges That Insecure Home Routers and "cloud" services Put Consumers' Privacy at Risk". Retrieved from: <https://www.ftc.gov/news-events/pressreleases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put>

³⁸ IoT Security Foundation. "UK Government moves towards regulating security in consumer IoT". Retrieved from: <https://www.iotsecurityfoundation.org/uk-government-moves-towards-regulating-security-inconsumer-iot>

Commissioner's Office (ICO) – imposed it based on 1.5 percent of BA's 2017 worldwide revenue.

It is difficult to estimate how breach of these regulations might fully impact an IoT security solution provider as a number of factors such as fiscal turnover, financial stability, and even business strategy will affect the result. In addition to financial penalties, providers may lose key personnel or suffer reputational damage which, in turn, may lead to negative effects on sales, share prices, and market trust.

EU Regulatory Frameworks at a glance

In European domain the main frameworks are:

- CE Marking
- General Data Protection Regulation (GDPR)
- Network and Information Security Directive (NIS Directive)

CE Marking ensures the safety, health, and environmental protections of products on the market in the EU³⁹. Applicable product categories and regulations may be updated at any time, underlining regulation's shifting landscape. CE marking and associated regulations may have direct impact on both the product (e.g. a device) and organization depending on the specific regulation. In addition, product manufacturers, importers and distributors are liable for ensuring compliance with CE Marking – particularly if the device is marketed under their name⁴⁰. In this case, IoT providers will need to obtain the appropriate information from the manufacturer to prove compliance. This may be difficult for distributors if the information is proprietary.

It is important for IoT providers and their supply chain to be aware of the manner in which the **EU's General Data Protection Regulation (GDPR)** applies to each organization⁴¹. Specific application of the regulation can vary by country, so local regulations should be reviewed when entering a marketplace within the EU. The regulation applies to data controllers and processors acting in the EU marketplace and/or handling personal information of EU residents and citizens. In an IoT environment the body responsible for compliance is likely to be the direct provider, such as a device provider (e.g. smart toy or refrigerator provider), utility provider (e.g. Internet service provider or electricity provider), or digital service provider (e.g. cloud services). In the IoT environment it is increasingly difficult to draw a line between data controllers and processors and may result in joint or dual designation – this risk is in addition to the increased liability for data processors implemented by GDPR. Data protection regulations are also applicable to product developers and manufacturers involved in the design and development of IoT products but not acting as an IoT provider. While GDPR does not make any specific requirements on technical or organizational security measures for compliance, it does present examples of 'appropriate' safeguards for specific provisions – such as encryption and

³⁹ European Commission. "CE Marking". Retrieved from: https://ec.europa.eu/growth/single-market/ce-marking_en

⁴⁰ Singapore. "Health Products Act". Retrieved from: <https://sso.agc.gov.sg/Act/HPA2007>

⁴¹ European Union. "General Data Protection Regulation". Retrieved from: <https://eur-lex.europa.eu/legalcontent/en/TXT/?uri=CELEX%3A32016R0679>

pseudonymisation. Safeguards are to be determined by the organization to ‘ensure a level of security appropriate to the risk’.

The **Network and Information Security Directive (NIS Directive)** applies only to those IoT providers designated as an Operator of Essential Services (OESs) – such as gas, electricity and water – and/or a Designated Service Provider (DSPs)⁴². In the IoT ecosystem, OESs are likely to be those providers working in areas like Smart Cities. Most other relevant IoT providers will fall under the DSP heading which includes online marketplaces, search engine, or cloud computing services. As with GDPR, an entity can be designated as both an OES and DSP. In some cases, DSPs have more explicit requirements regarding incident response and reporting.

⁴² Hill, Kashmir and Surya Mattu. “The House That Spied on Me” Williams, Kevin. Gizmodo, July 2, 2018. Retrieved from: <https://gizmodo.com/the-house-that-spied-on-me-1822429852>

7 Conclusions

C4IIoT is addressing a crucial problem that affects a wide range of enterprises across the globe: malicious attacks to IoT systems with high economic and social impact, especially in the manufacturing domain. To reduce the risks and improve the general security of IoT and IIoT environments, there is a need for an end-to-end approach to cybersecurity. C4IIoT provides a holistic approach that orchestrates heterogeneous tools to offer high levels of protection.

The market analysis shows that IoT security market is projected to grow at an impressive CAGR of more than 35%, on account of increasing number of connected devices in the IoT landscape and growing awareness among governments and enterprises regarding cyberattacks. This trend is an obvious opportunity for C4IIoT to take advantage the revealed key challenges and market drivers towards a holistic customer value approach by establishing capabilities to support business modelling for each market.

However, the competition seems to be rough as IoT cybersecurity becomes more and more attractive for traditional players and start-ups as well. Regulatory and policy maker bodies support the incentives schemes towards products/services and the creation of an ecosystem addressing security vulnerabilities and the creation of a secure environment in align with industry 4 principles. But much work has to be done in the field of regulation and standardization as already pointed out. These factors impede the effective management of interoperability and scalability issues of end to end solutions and stakeholders should be approached with these aspects in mind.

Finally, a preliminary business model was formulated to describe, design, challenge, and pivot potential C4IIoT business model. With Business Model Canvas we visualize the elements that describes C4IIoT value proposition, infrastructure, customers, and finances in order to align future activities and potential trade-offs. In any case, this market analysis will be revised, feeding with updated market dynamics the final business model to be adopted.

ANNEX

Below are initial versions of SWOT Analysis (Strengths, Weaknesses, Opportunities, Threats) considering c4iiot solution as a whole from industrial partners of C4IIoT Consortium.

STRENGTHS

THALES	➤ The solution can support a possible massive deployment of IIoTs.
VIP	<ul style="list-style-type: none"> ➤ Big network of IoT partners on different verticals ➤ International and regional presence through A1 group of companies ➤ IoT global platform for connectivity and device management ➤ Strong level of network security
ITML	➤ Addressing an evolving market with significant challenges in cybersecurity
Sphynx	<ul style="list-style-type: none"> ➤ Holistic, end-to-end provision of security tailored to the intricacies of Industry 4.0. ➤ Consortium know-how spanning heterogeneous technologies and domains
Infineon	<ul style="list-style-type: none"> ➤ Holistic platform ➤ Practical testbed
IBM	<ul style="list-style-type: none"> ➤ Privacy-aware access management solution ➤ Elements of decentralization
STS	<ul style="list-style-type: none"> ➤ Holistic, end-to-end provision of security tailored to the intricacies of Industry 4.0. ➤ Consortium know-how spanning heterogeneous technologies and domains

WEAKNESSES

THALES	➤ The solution could not be adopted by all the manufacturing community.
VIP	<ul style="list-style-type: none"> ➤ Identifying all risks related to security ➤ Implementing end to end IoT security brings a lot of challenges: HW level, application level, network level
ITML	➤ N/A
Sphynx	<ul style="list-style-type: none"> ➤ Complex canvas of technologies from different partners that may be hard to integrate and offer in a usable manner. ➤ Lack of leading position in the market
Infineon	<ul style="list-style-type: none"> ➤ Insufficient standardization due to the novelty of the solution ➤ Not-enough blockchain experience
IBM	➤ Integrating Blockchain into the world of IIoT may introduce scalability challenges
STS	<ul style="list-style-type: none"> ➤ Complex canvas of technologies from different partners, that may be hard to integrate and offer in a usable manner. ➤ Lack of leading position in the market

OPPORTUNITIES

THALES	➤ As an industrial partner, the project offers the possibility to address new market sectors especially in Manufacturing sector.
VIP	<ul style="list-style-type: none"> ➤ Fastest growing segment in telco offering (services) ➤ New products and services that could be offered to the partners/customers ➤ To gain new knowledge and practice related to security in IoT aspects
ITML	<ul style="list-style-type: none"> ➤ Smart manufacturing evolving fast in the last years ➤ Implementations of IoT in industrial environments are growing fast
Sphynx	<ul style="list-style-type: none"> ➤ Alleviate security concerns in Industry 4.0 applications, enabling the exploitation of their full potential. ➤ Enable the provision of Security as a Service or other novel business models for the provision of security in the context of Industry 4.0 ➤ Lack of established security frameworks in the domain
Infineon	<ul style="list-style-type: none"> ➤ Spread HW Security usage in IIoT. ➤ Increase blockchain expertise in the IIoT domain.
IBM	➤ Combining Blockchain technology and its advantages with the fast-growing domain of IIoT
STS	<ul style="list-style-type: none"> ➤ Alleviate security concerns in Industry 4.0 applications, enabling the exploitation of their full potential ➤ Enable the provision of Security as a Service or other novel business models for the provision of security in the context of Industry 4.0 ➤ Lack of established security frameworks in the domain

THREATS

THALES	<ul style="list-style-type: none"> ➤ A major unexpected cybersecurity issue could have catastrophic consequences in the industrial domain and therefore be a brake to the solution brought by the project. ➤
VIP	<ul style="list-style-type: none"> ➤ Lack of IoT security regulations and standards on global market ➤ Security breach of devices and applications. ➤ Privacy data leaks ➤
ITML	<ul style="list-style-type: none"> ➤ Rapid technology advancements that can overcome C4IIOT approach within the project's duration. ➤
Sphynx	<ul style="list-style-type: none"> ➤ Failure to create a solution adaptable to the different heterogeneous environments comprising Industry 4.0 ➤ Not follow the high-stakes and ever-changing threat landscape ➤ Competitors
Infineon	➤ Potential bugs and scalability issues due to the usage of state-of-the-art concepts.
IBM	➤ Risk of private keys theft or mismanagement
STS	<ul style="list-style-type: none"> ➤ Failure to create a solution adaptable to the different heterogeneous environments comprising Industry 4.0 ➤ Not follow the high-stakes and ever-changing threat landscape